Algebraic geometry, Gröbner bases, and Normalization

Janko Boehm
boehm@mathematik.uni-kl.de

University of Kaiserslautern

14.10.2014

Algebraic Varieties

Algebraic Varieties

Let K be a field. An **affine algebraic variety** is the common zero-set

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

of polynomials $f_1, ..., f_r \in K[x_1, ..., x_n]$.

Algebraic Varieties

Let K be a field. An **affine algebraic variety** is the common zero-set

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

of polynomials $f_1, ..., f_r \in K[x_1, ..., x_n]$.

Example

- $V(1) = \emptyset$, $V(0) = K^n$,

Algebraic Varieties

Let K be a field. An **affine algebraic variety** is the common zero-set

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

of polynomials $f_1, ..., f_r \in K[x_1, ..., x_n]$.

Example

- $V(1) = \emptyset$, $V(0) = K^n$,
- the set of solutions of a linear system of equations

$$A \cdot x - b = 0$$

Algebraic Varieties

Let K be a field. An **affine algebraic variety** is the common zero-set

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

of polynomials $f_1, ..., f_r \in K[x_1, ..., x_n]$.

Example

- $V(1) = \emptyset$, $V(0) = K^n$,
- the set of solutions of a linear system of equations

$$A \cdot x - b = 0$$

- the graph

$$\Gamma(g) = V\left(x_2 \cdot b(x_1) - a(x_1)\right) \subset K^2$$

  of a rational function

$$g = \frac{a}{b} \in K(x_1)$$

Examples of Varieties: Graphs

Examples of Varieties: Graphs

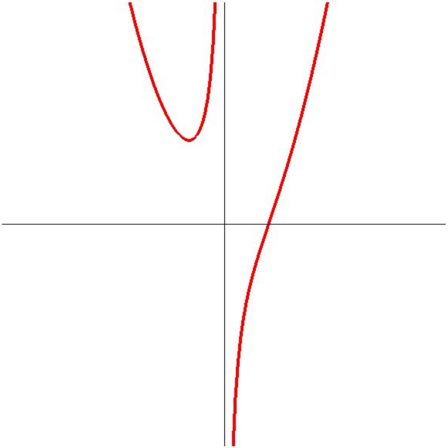
The graph of $g(x_1) = \frac{x_1^3 - 1}{x_1}$ is

$$V(x_2 x_1 - x_1^3 + 1) \subset K^2$$

Examples of Varieties: Graphs

The graph of $g(x_1) = \frac{x_1^3 - 1}{x_1}$ is

$$V(x_2 x_1 - x_1^3 + 1) \subset K^2$$



Examples of Varieties: Curves

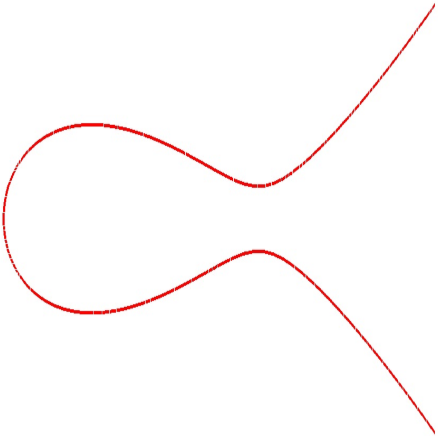
Not every curve in K^2 is a graph, e.g., the **elliptic curve**

$$V(x_2^2 - x_1^3 - x_1^2 + 2x_1 - 1)$$

Examples of Varieties: Curves

Not every curve in K^2 is a graph, e.g., the **elliptic curve**

$$V(x_2^2 - x_1^3 - x_1^2 + 2x_1 - 1)$$

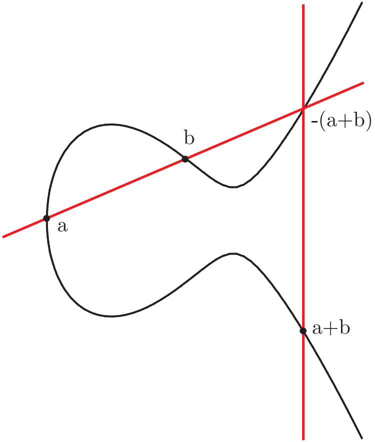


Examples of Varieties: Curves

Elliptic curves come with a group structure. They play an important role in Number Theory and Cryptography (e.g. Diffie-Hellman key exchange).

Examples of Varieties: Curves

Elliptic curves come with a group structure. They play an important role in Number Theory and Cryptography (e.g. Diffie-Hellman key exchange).



Examples of Varieties: Surfaces

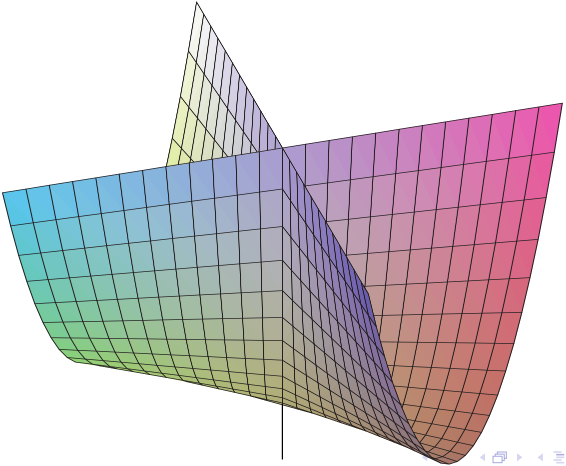
There are also varieties of higher dimension, e.g., **Whitney's umbrella**

$$V(y^2 - x^2 z)$$

Examples of Varieties: Surfaces

There are also varieties of higher dimension, e.g., **Whitney's umbrella**

$$V(y^2 - x^2 z)$$



Examples of Varieties: Cubic Surfaces

Theorem (Cayley, 1848)

Any projective smooth cubic surface over $\mathbb{C}$ contains exactly 27 lines.

Examples of Varieties: Cubic Surfaces

Theorem (Cayley, 1848)

Any projective smooth cubic surface over $\mathbb{C}$ contains exactly 27 lines.

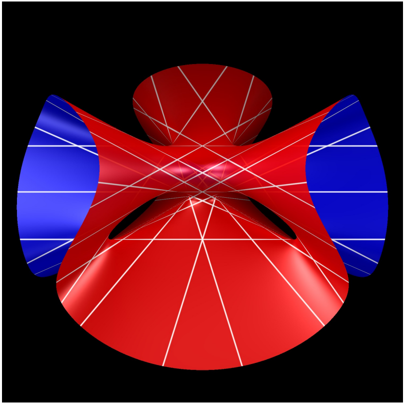
The **Clebsch Cubic** [Clebsch, 1871] has 27 real lines:

Examples of Varieties: Cubic Surfaces

Theorem (Cayley, 1848)

Any projective smooth cubic surface over $\mathbb{C}$ contains exactly 27 lines.

The **Clebsch Cubic** [Clebsch, 1871] has 27 real lines:



Examples of Varieties: Splines

The cubic spline $C \subset K^2$ parametrized by

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

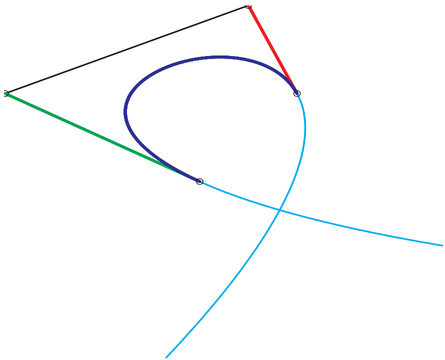
with $t \in [0,1]$ passes through the points $(p_0, q_0), (p_3, q_3) \in K^2$ and the tangents at these points through (p_1, q_1) and (p_2, q_2).

Examples of Varieties: Splines

The cubic spline $C \subset K^2$ parametrized by

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

with $t \in [0,1]$ passes through the points $(p_0, q_0), (p_3, q_3) \in K^2$ and the tangents at these points through (p_1, q_1) and (p_2, q_2).

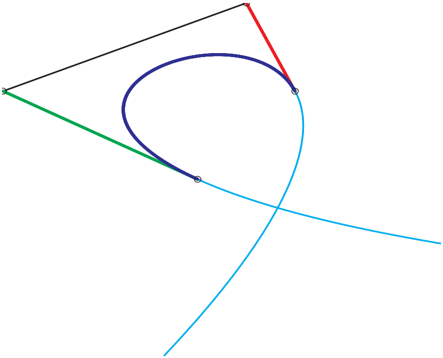


Examples of Varieties: Splines

The cubic spline $C \subset K^2$ parametrized by

$$x_1(t) = p_0(1-t)^3 + 3p_1 t(1-t)^2 + 3p_2 t^2(1-t) + p_3 t^3$$
$$x_2(t) = q_0(1-t)^3 + 3q_1 t(1-t)^2 + 3q_2 t^2(1-t) + q_3 t^3$$

with $t \in [0,1]$ passes through the points $(p_0, q_0), (p_3, q_3) \in K^2$ and the tangents at these points through (p_1, q_1) and (p_2, q_2).



The curve sector C is a subset of an algebraic curve $\overline{C}$.

$\overline{C}$ is the closure of C in the **Zariski Topology**, which has as closed sets the algebraic varieties.

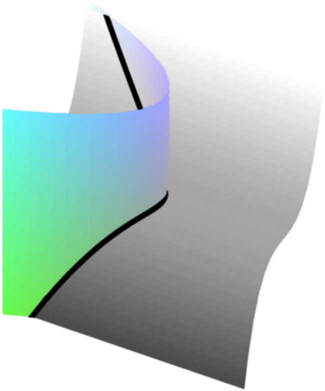
Projections

By projecting a smooth curve in K^3 (here the so called **twisteted cubic**) one may obtain a singular curve:

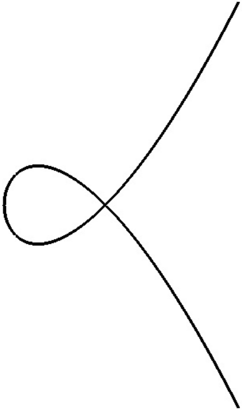
Projections

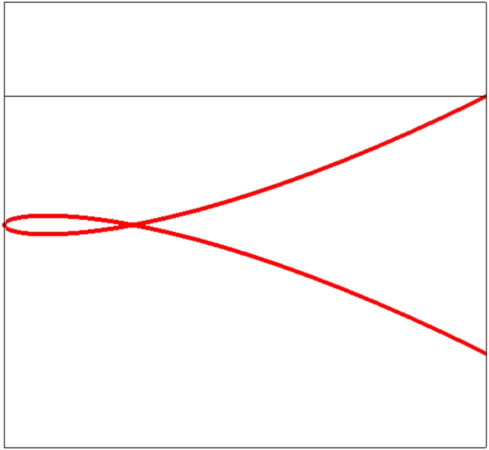
By projecting a smooth curve in K^3 (here the so called **twisteted cubic**) one may obtain a singular curve:

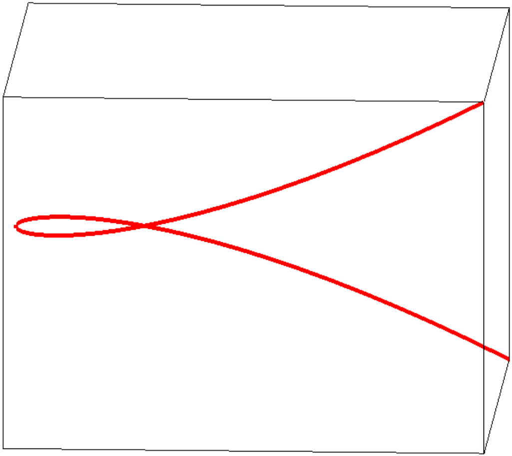
$V(y - x^2, z - x^3)$

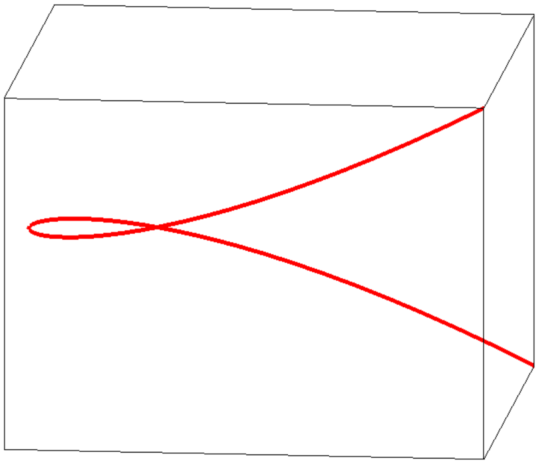


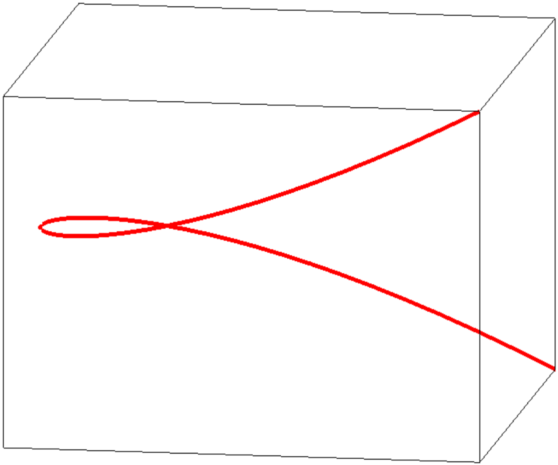
$\longrightarrow$

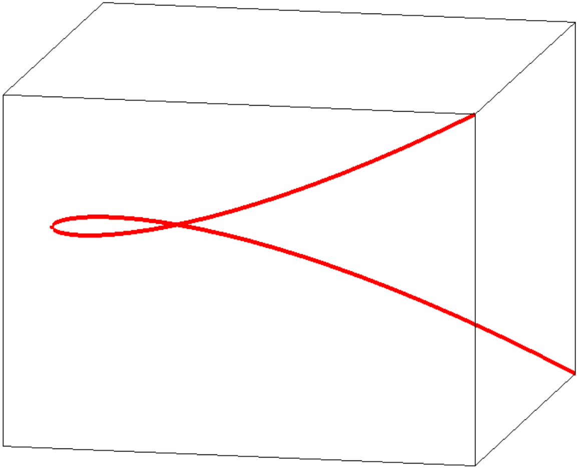


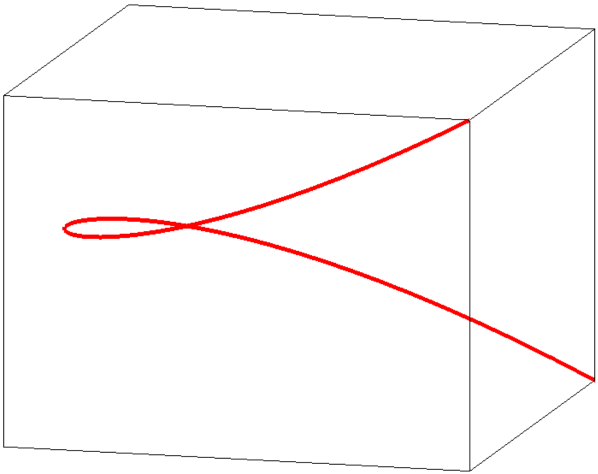


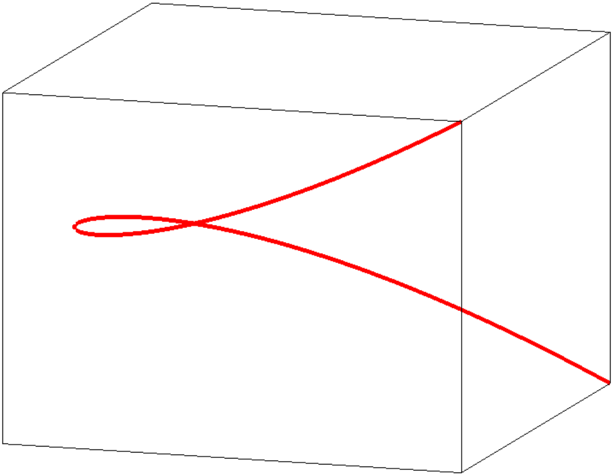


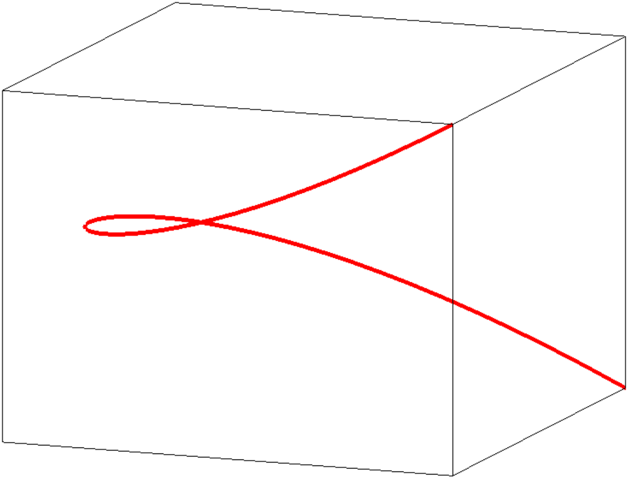


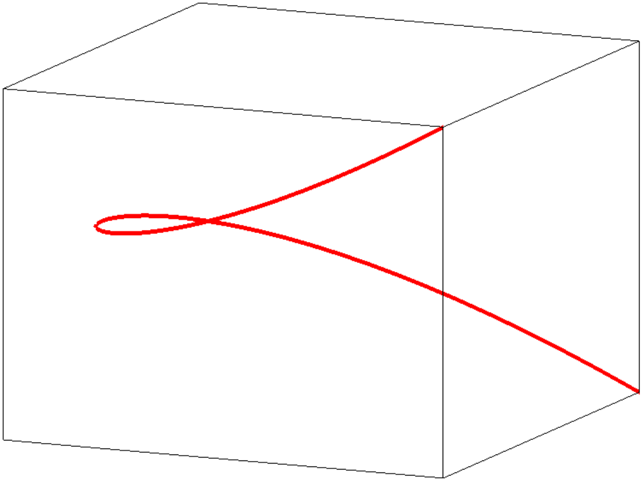


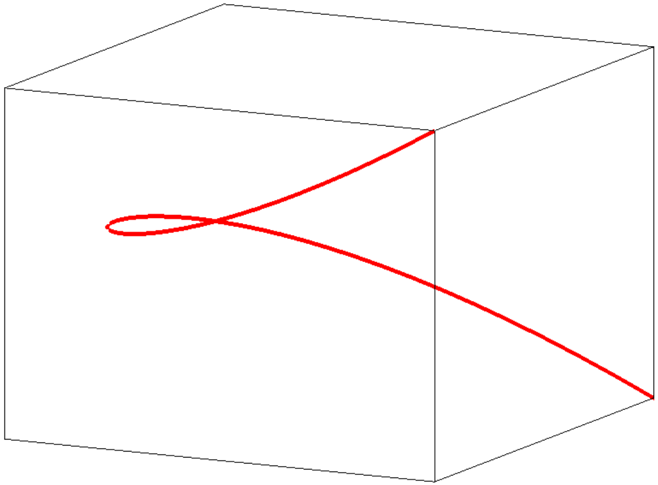


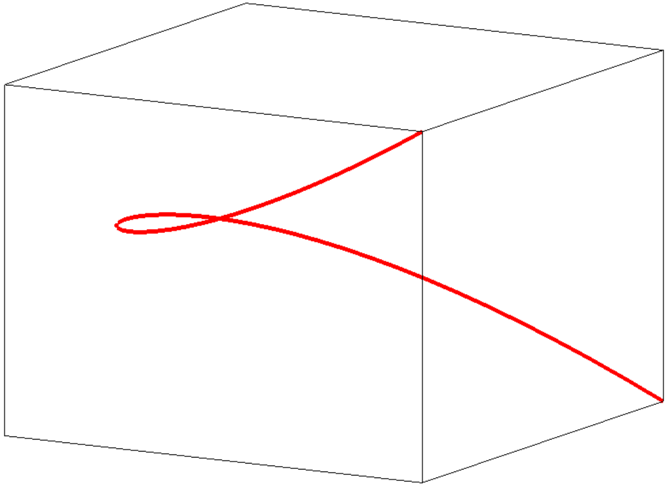


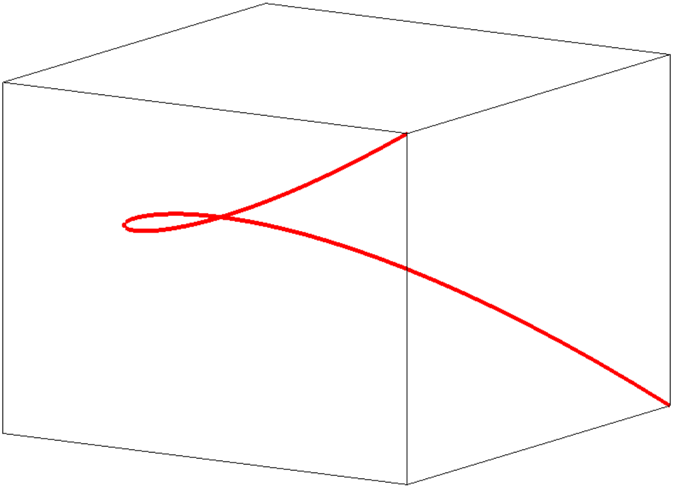


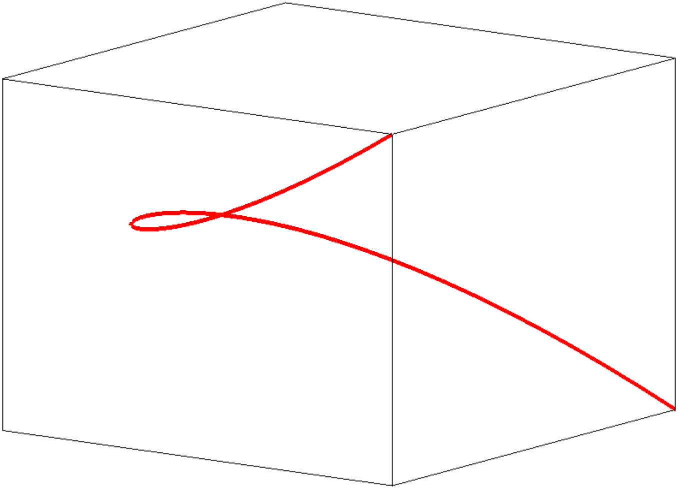


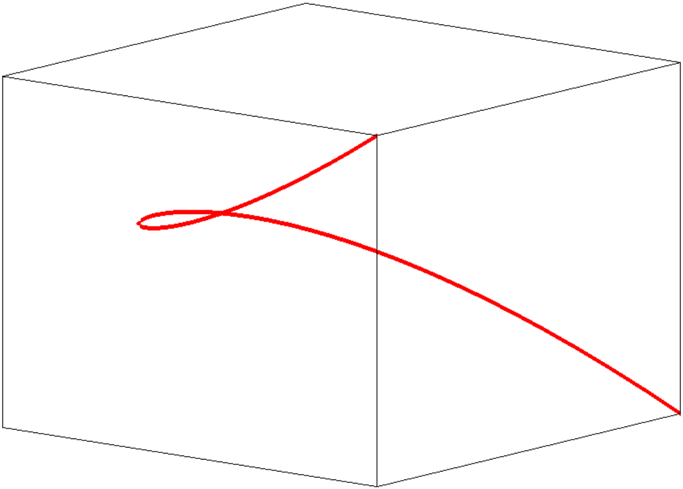


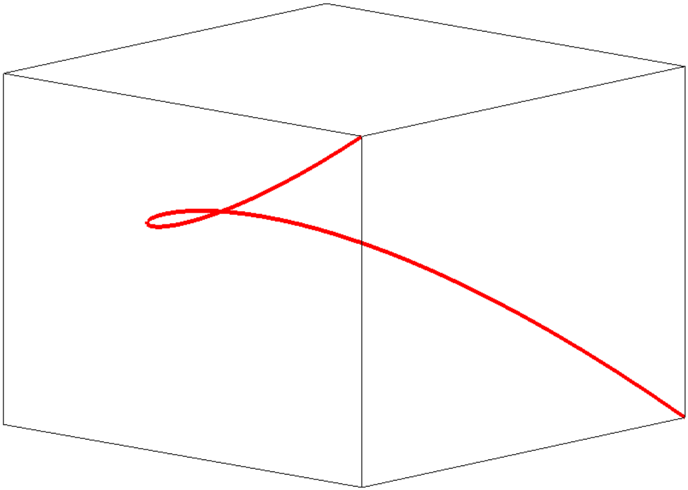


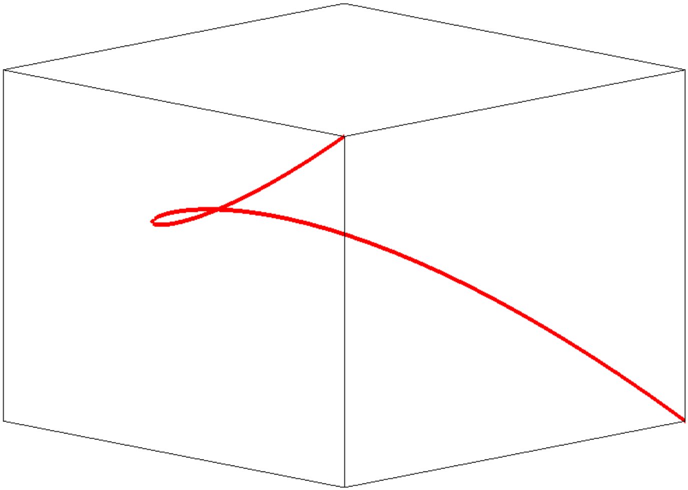


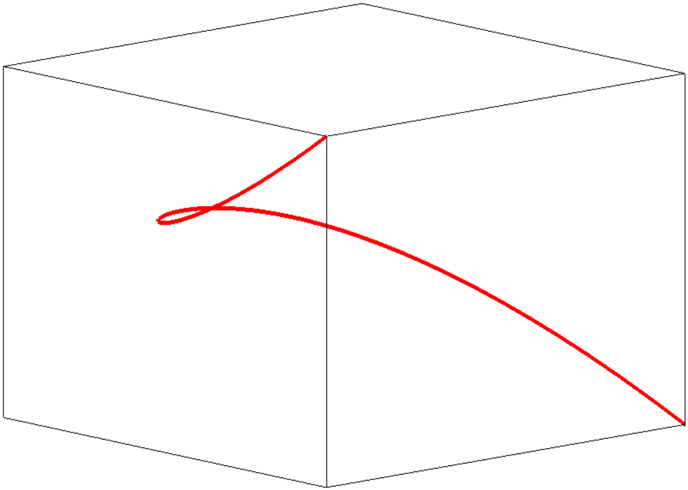


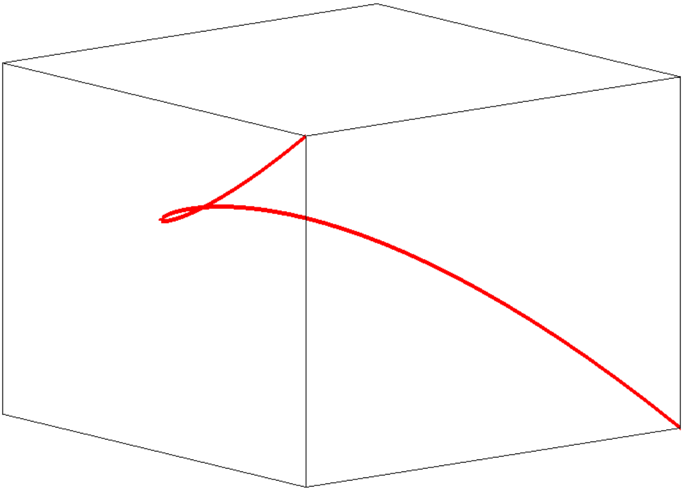


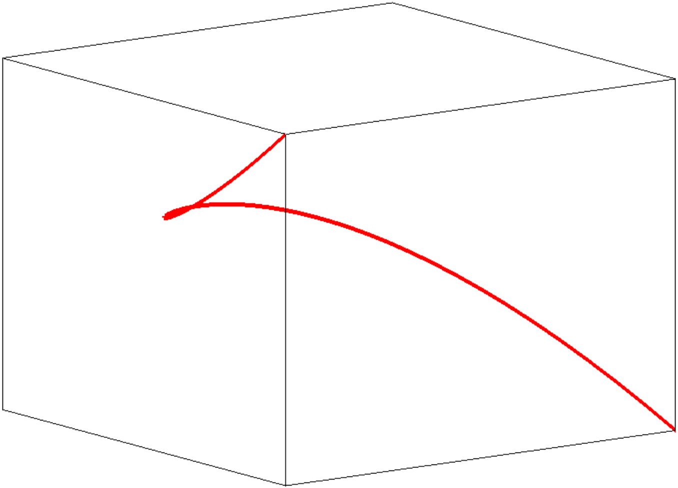


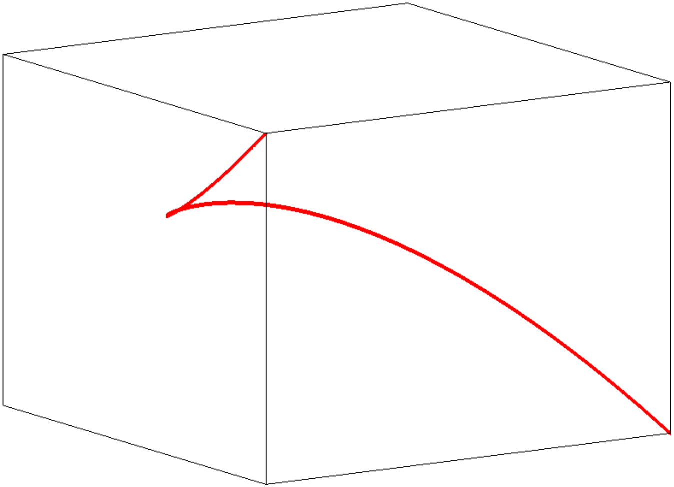


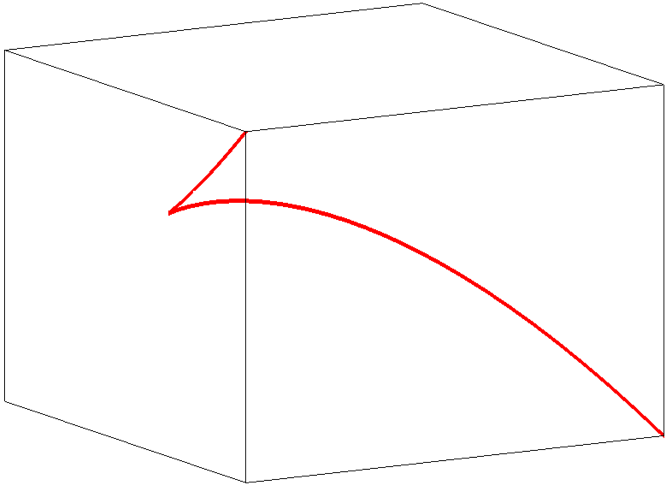


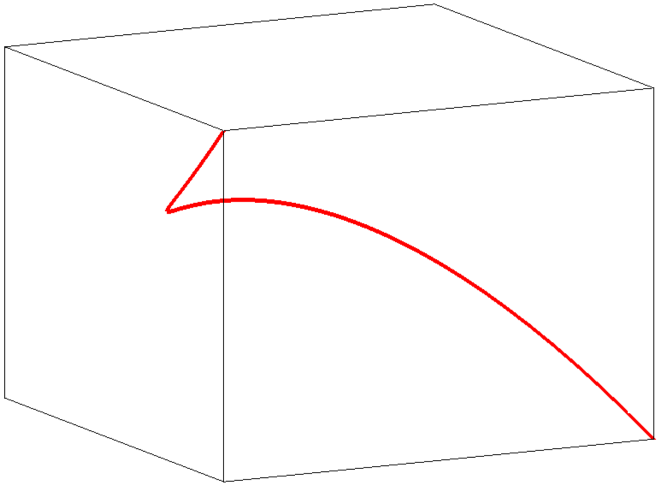


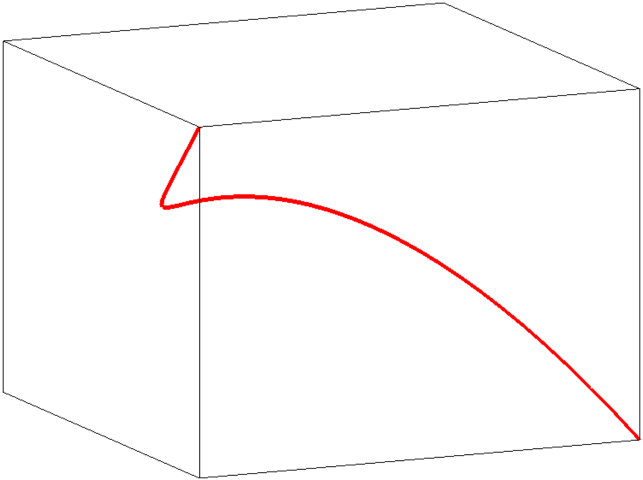


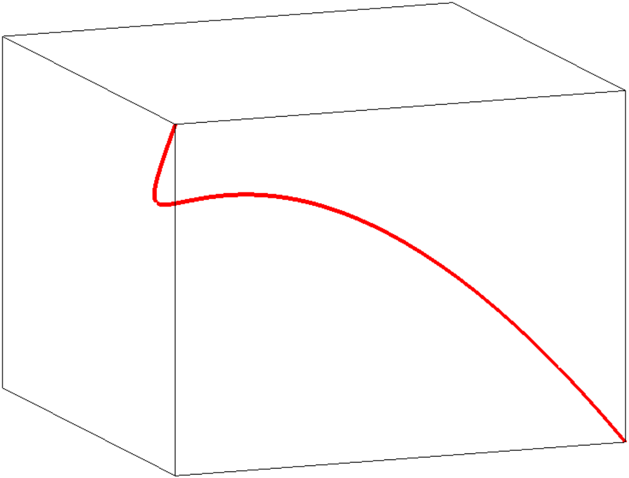


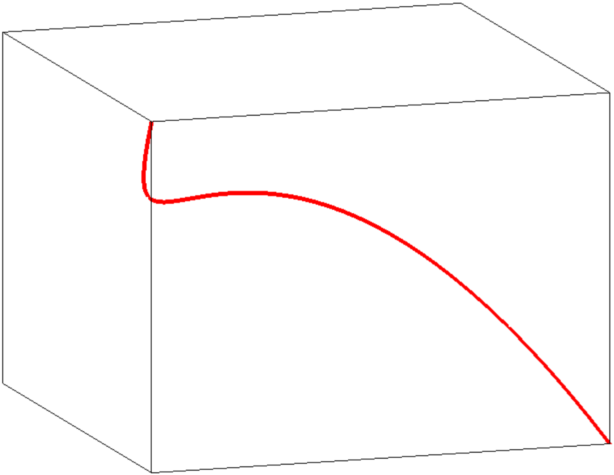


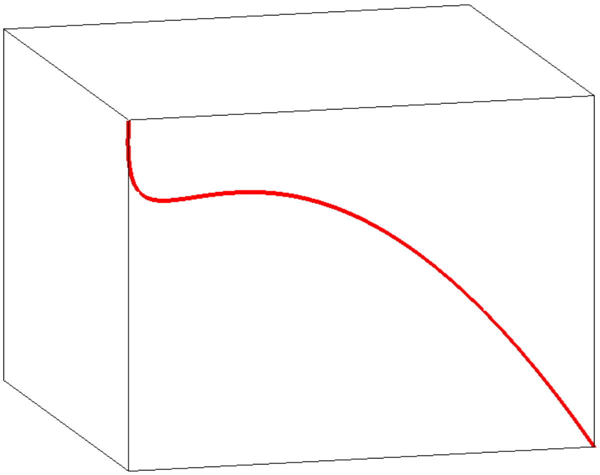


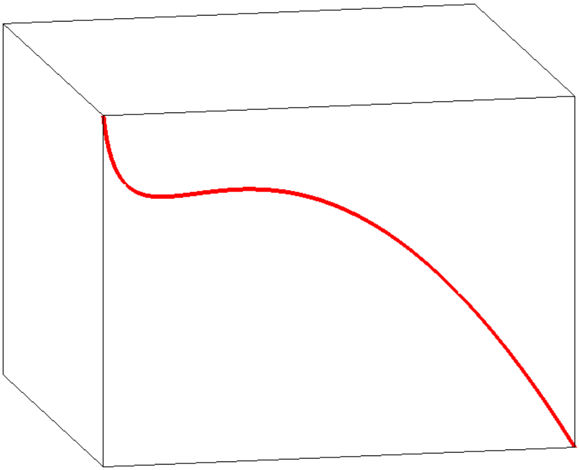


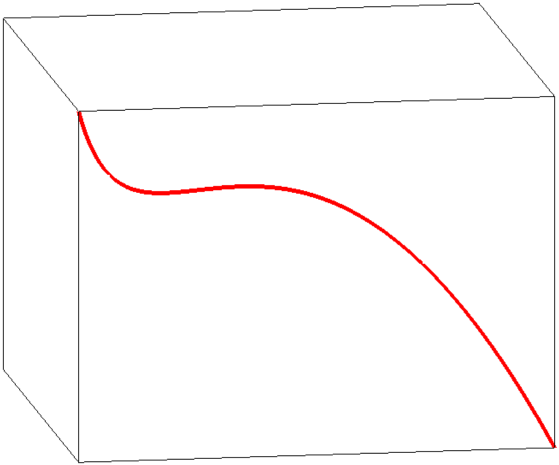


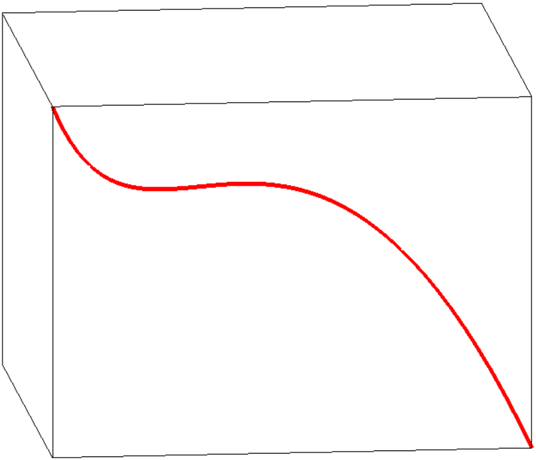


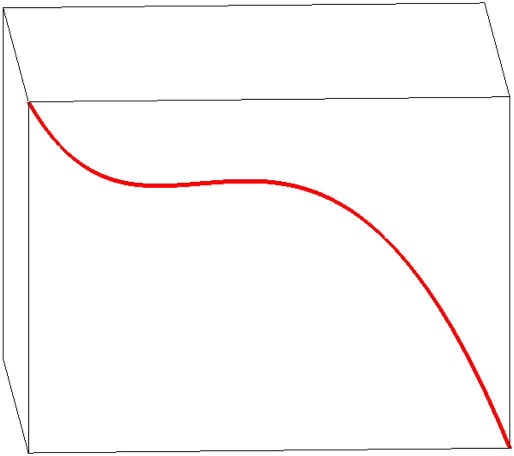


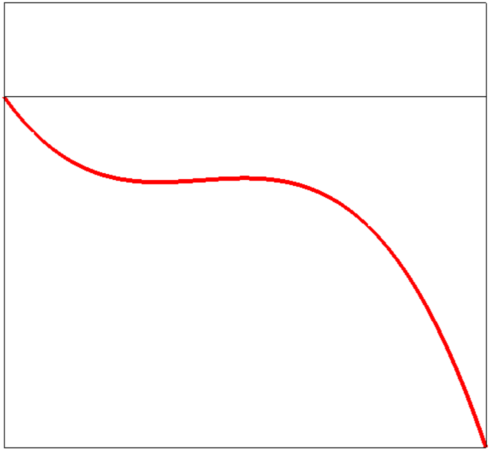


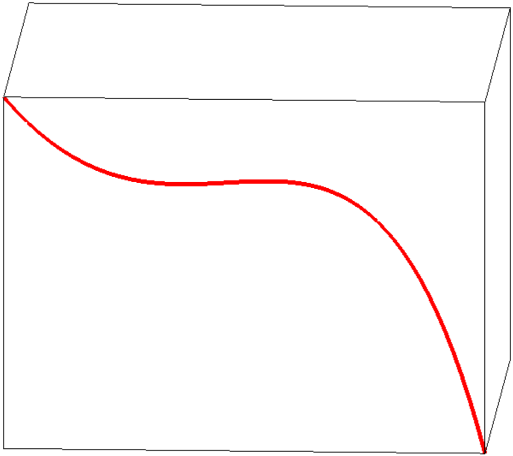


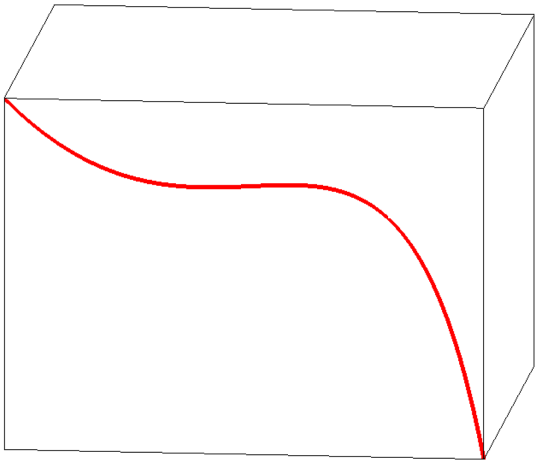


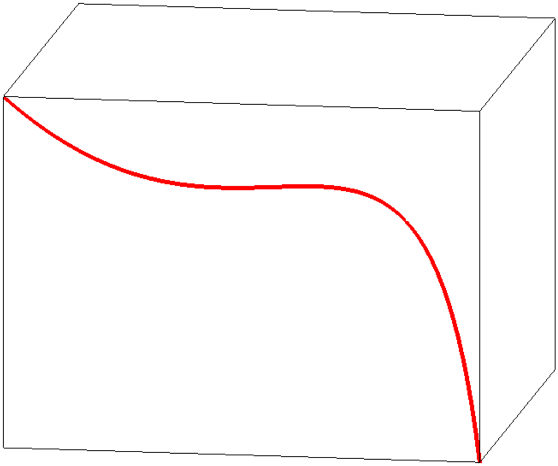


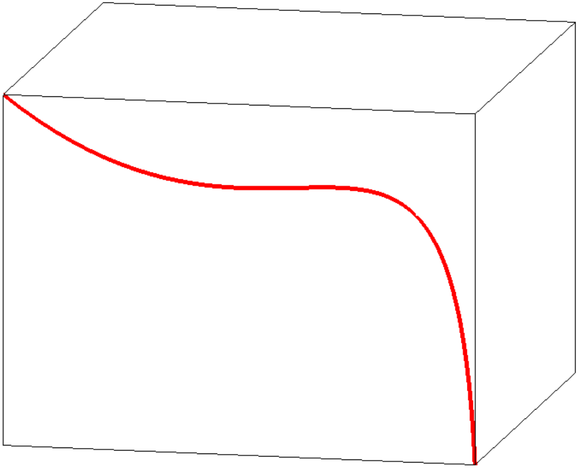


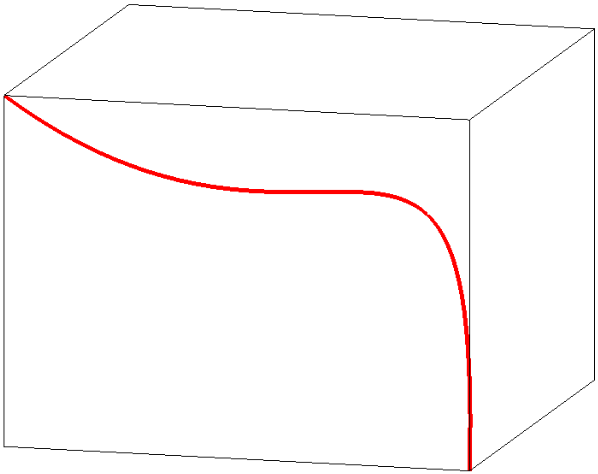


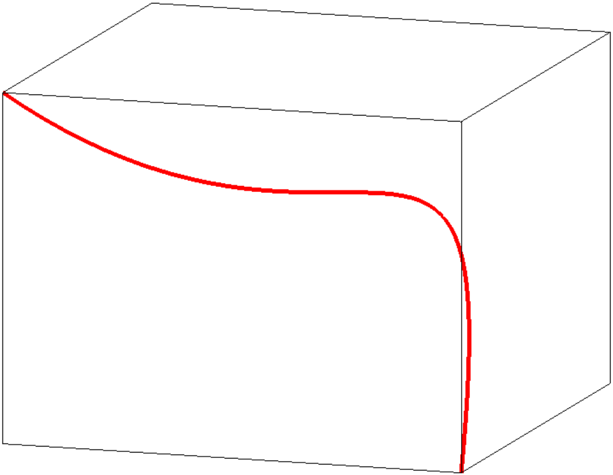


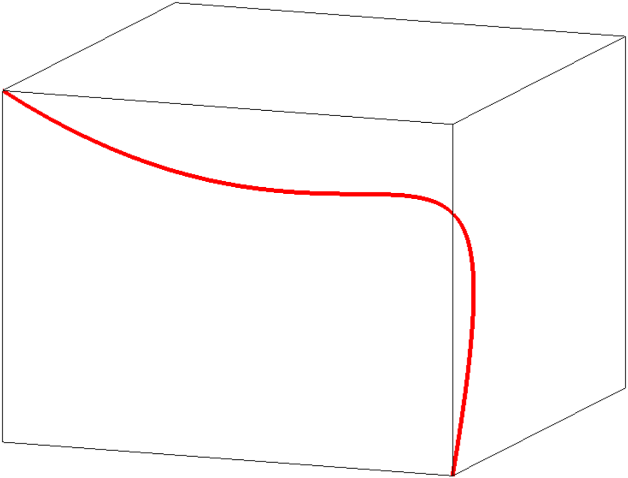


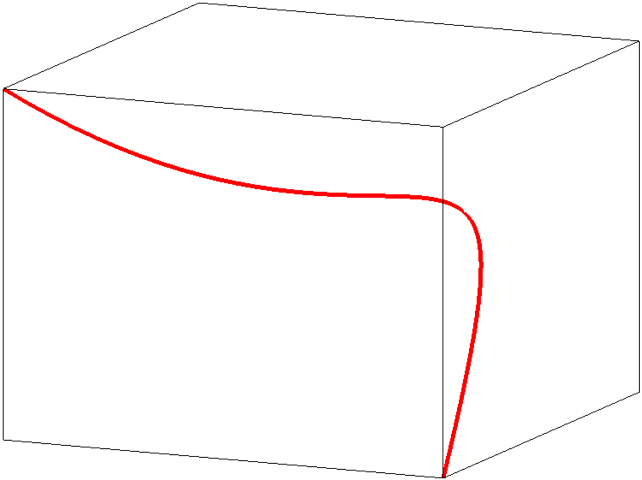


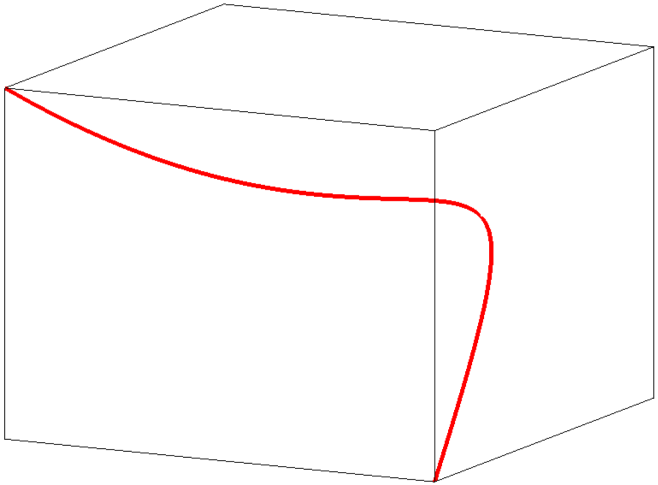


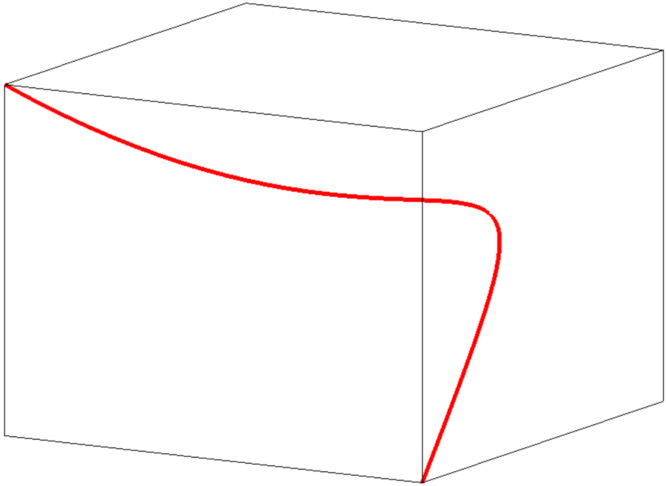


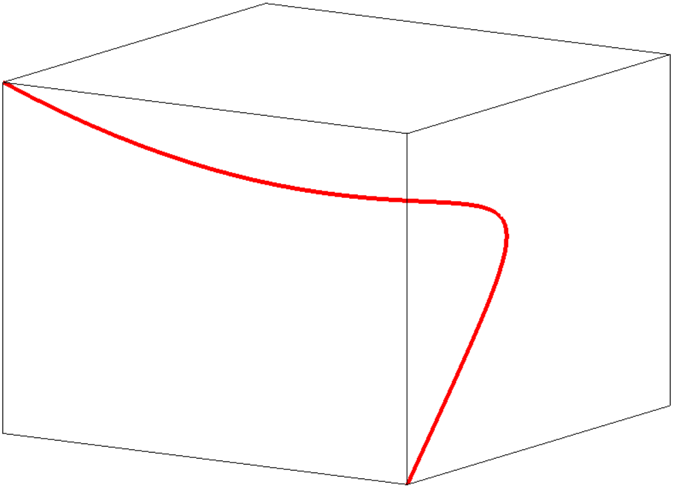


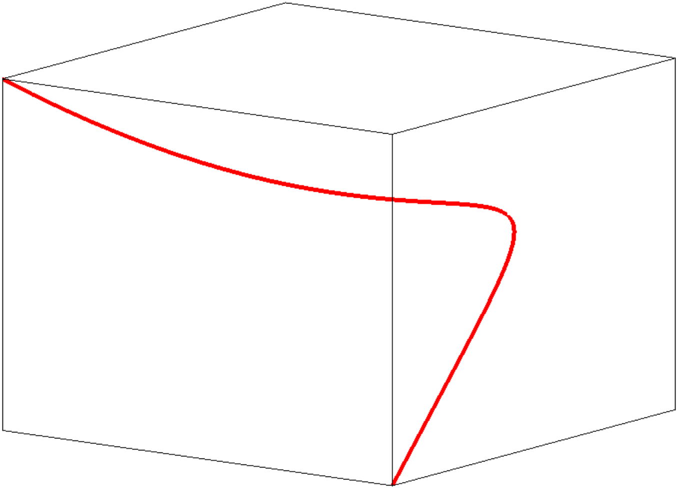


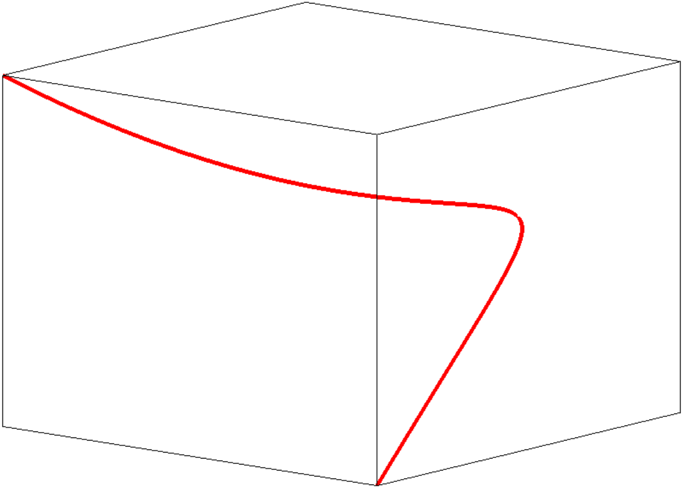


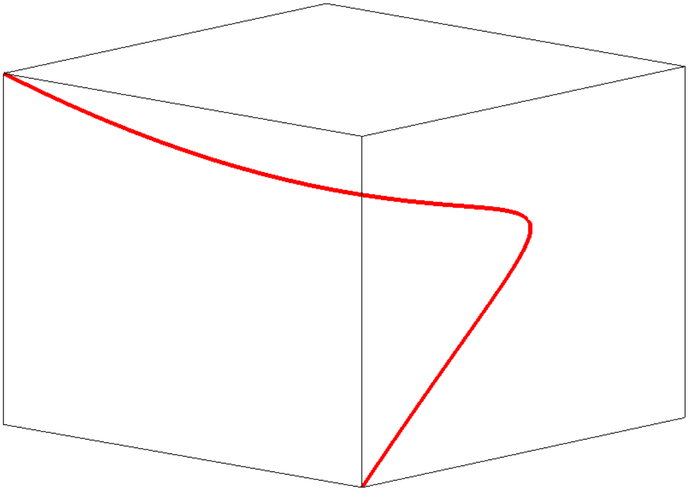


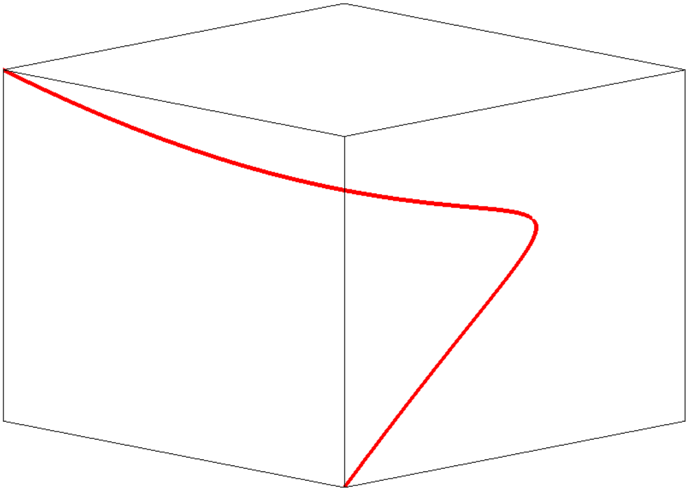


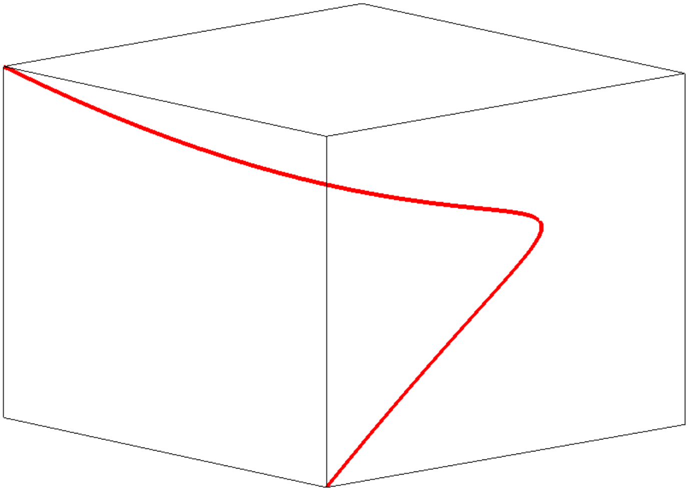


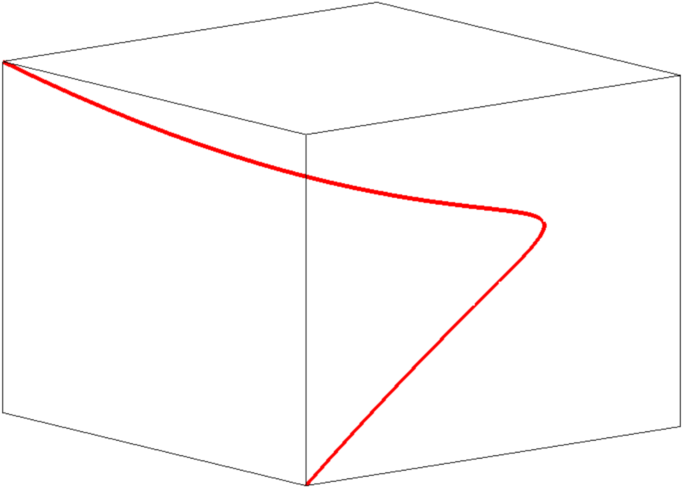


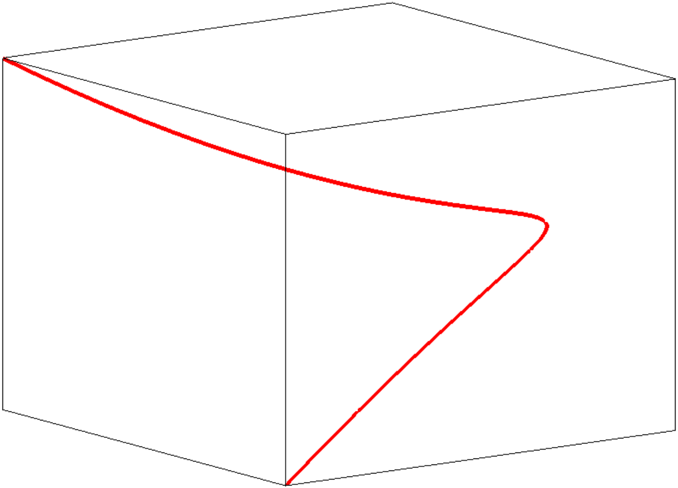


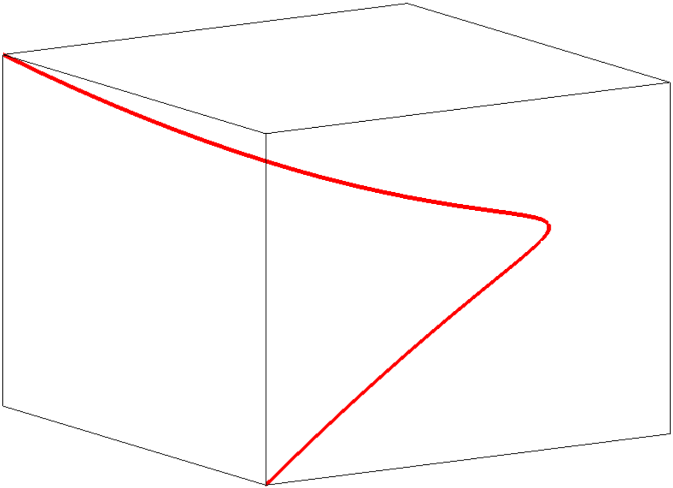


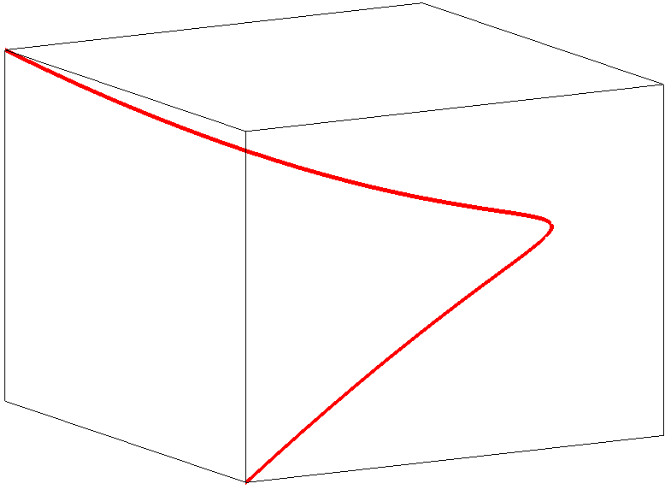


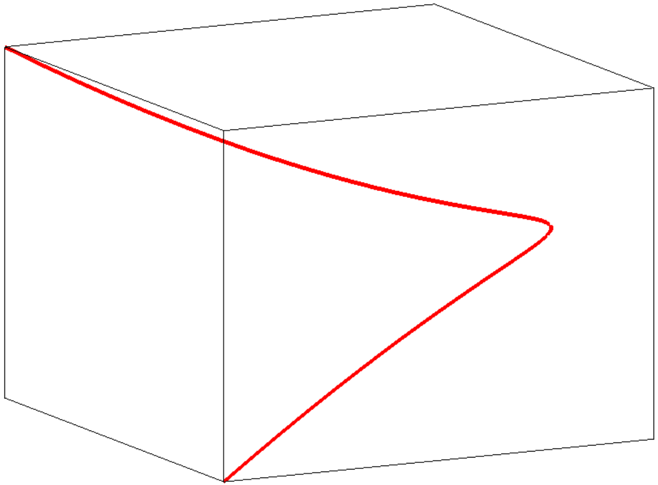


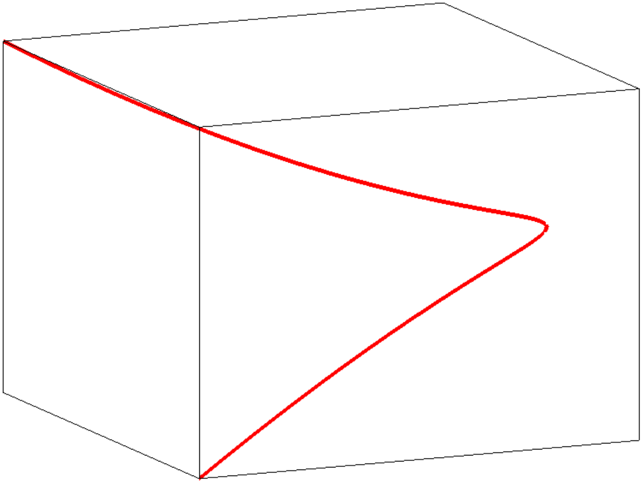


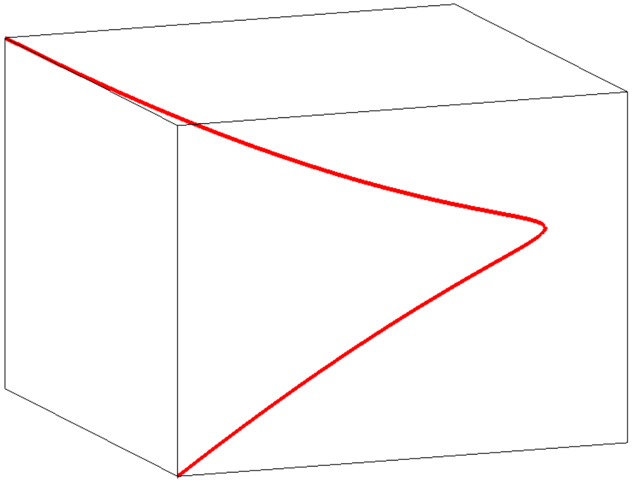


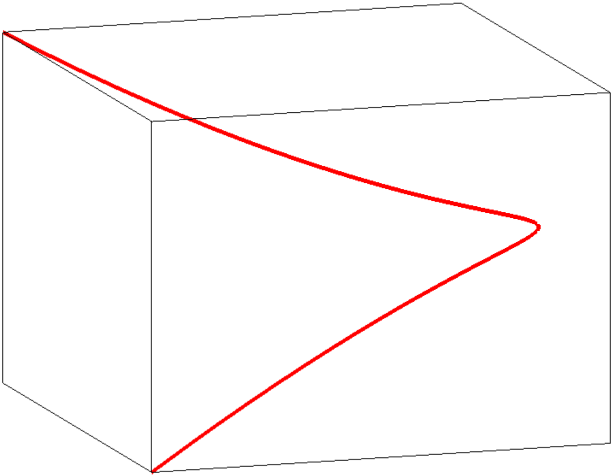


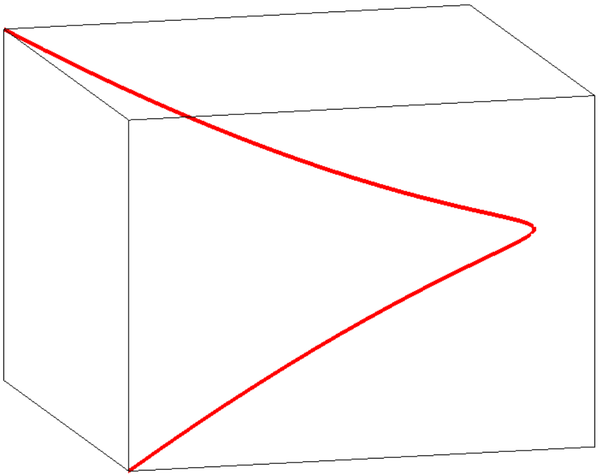


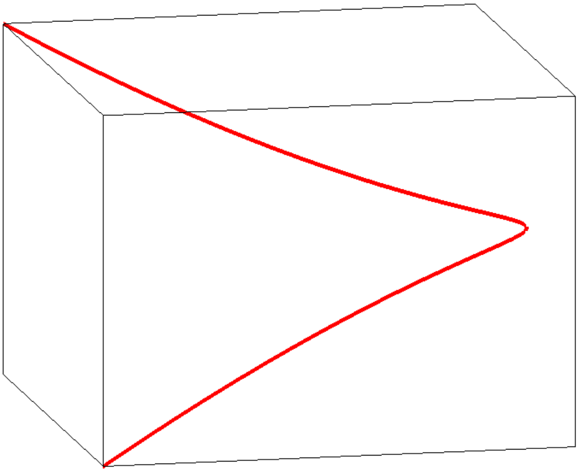


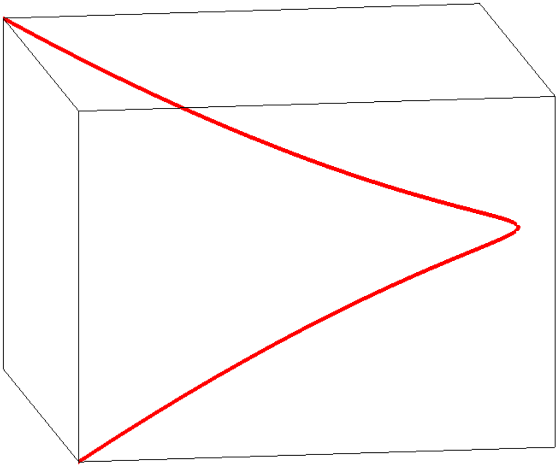


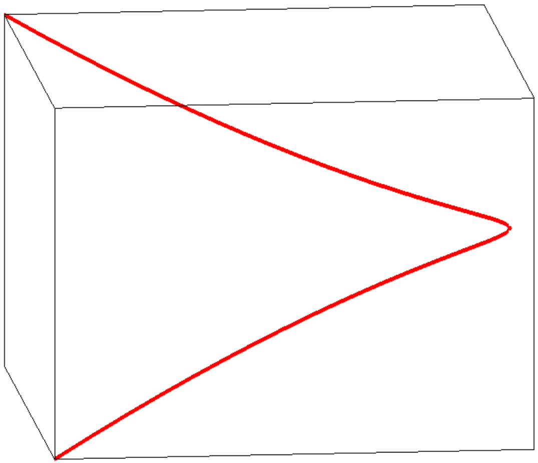


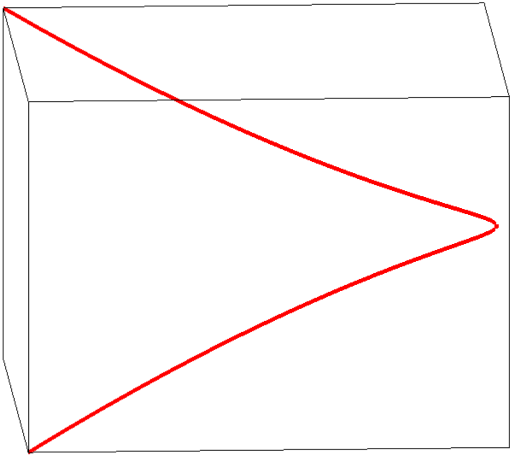


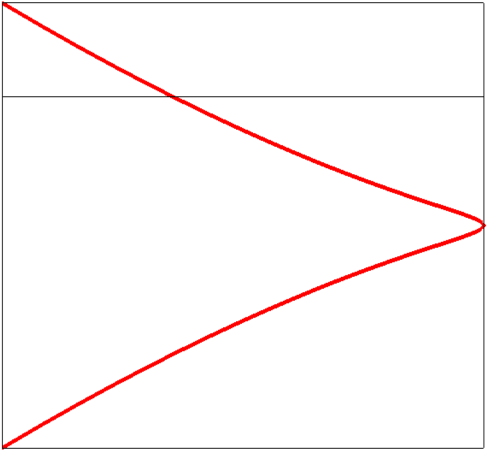


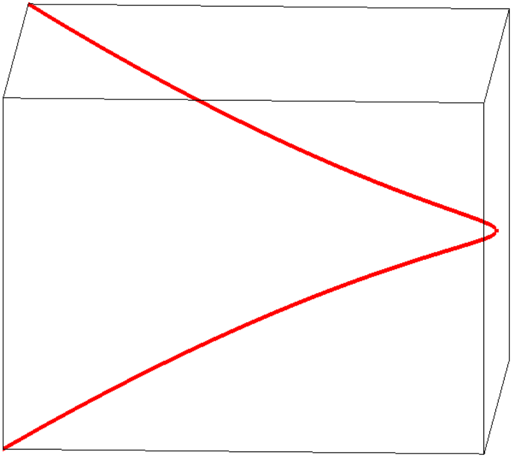


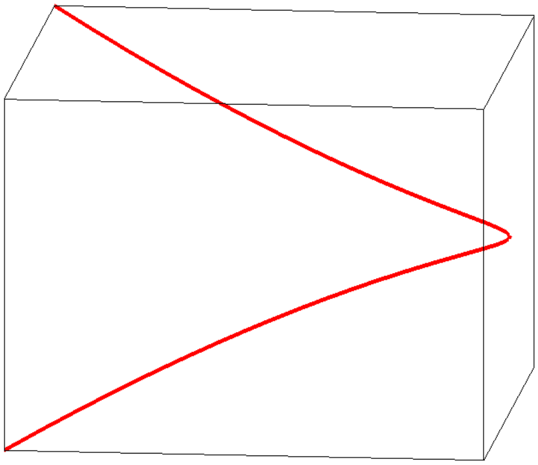


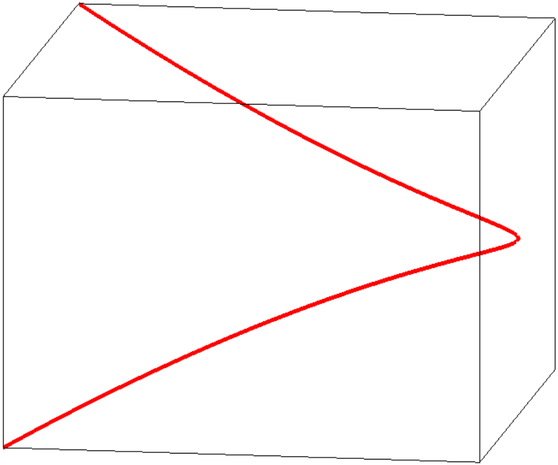


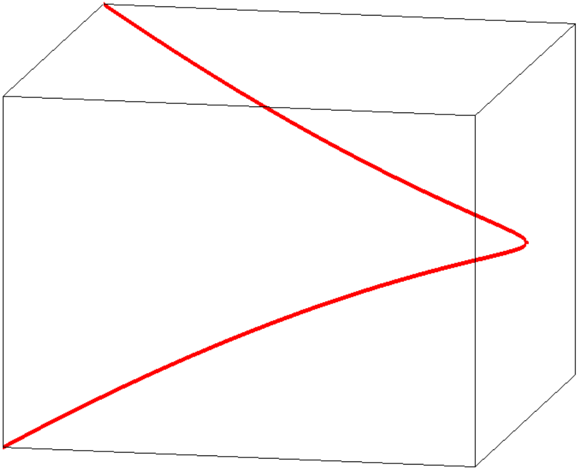


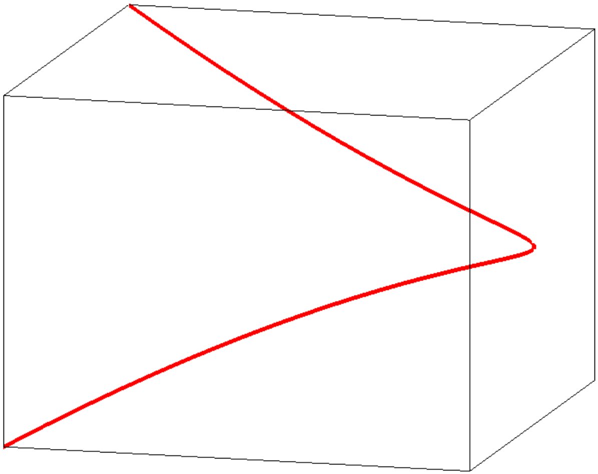


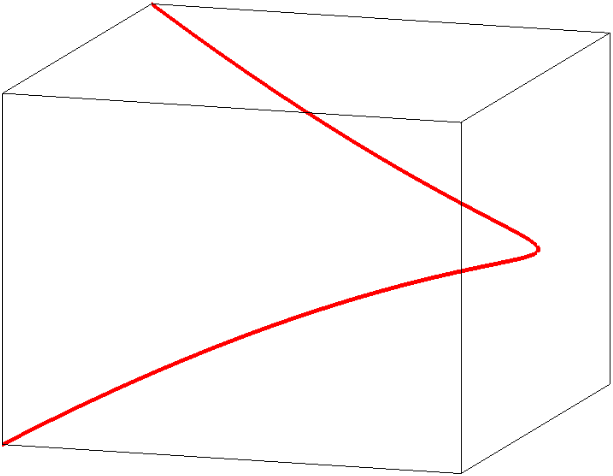


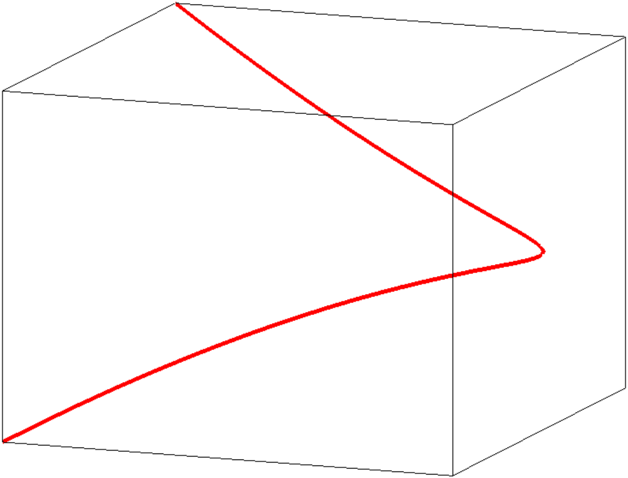


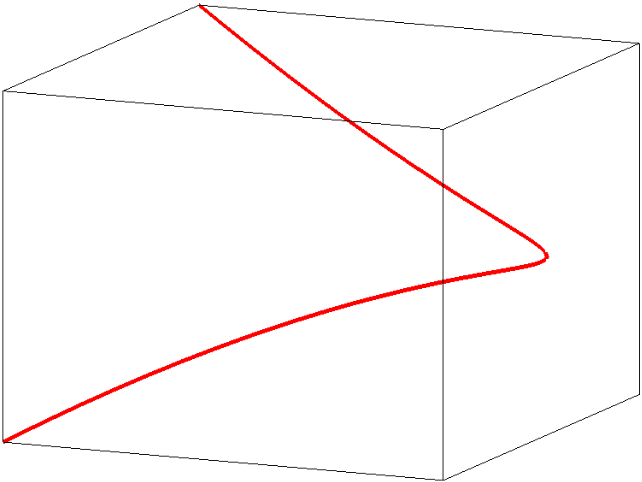


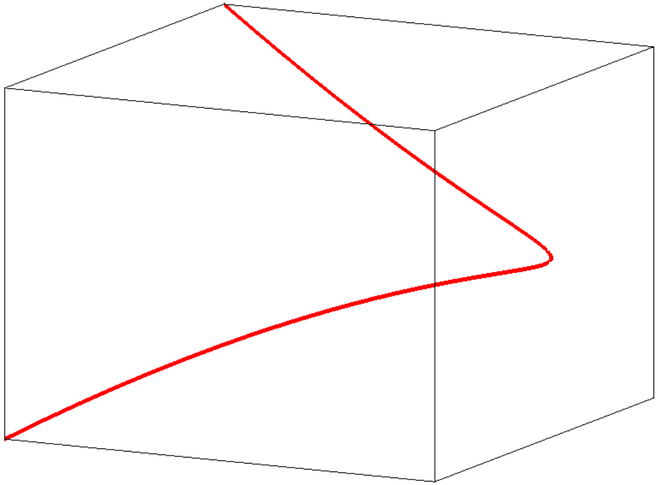


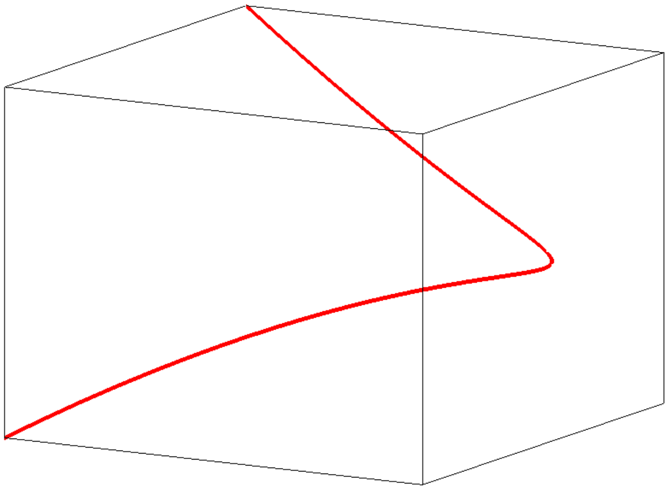


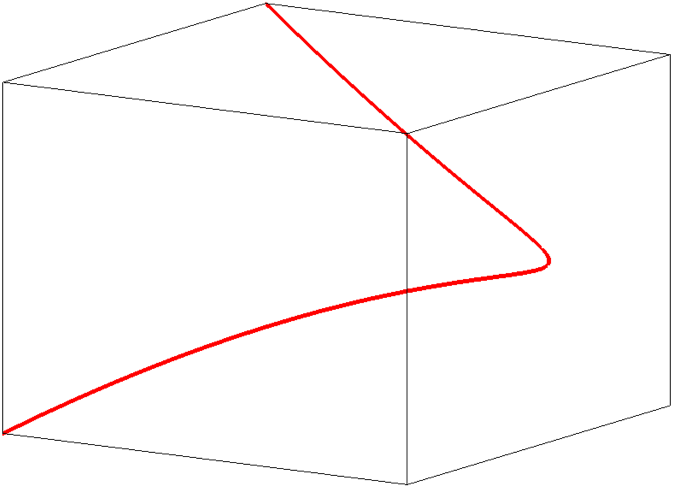


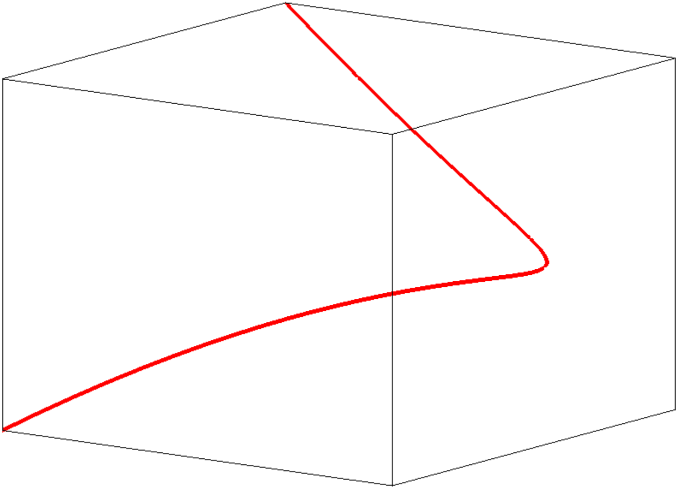


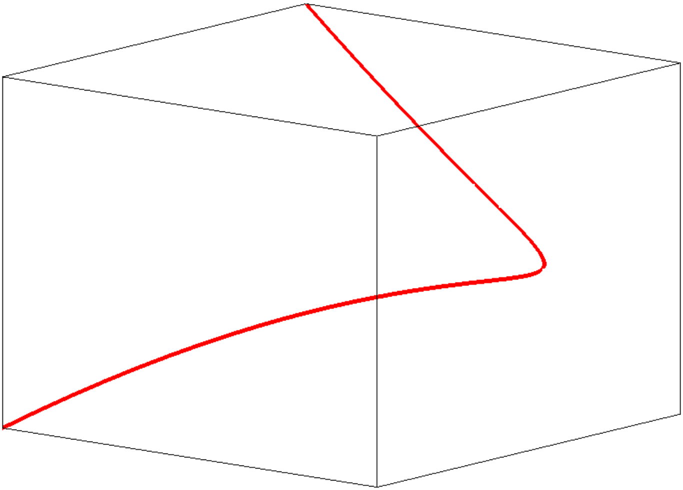


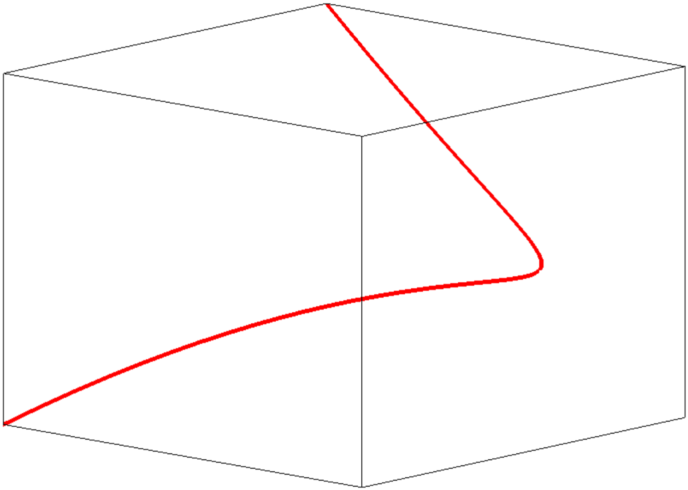


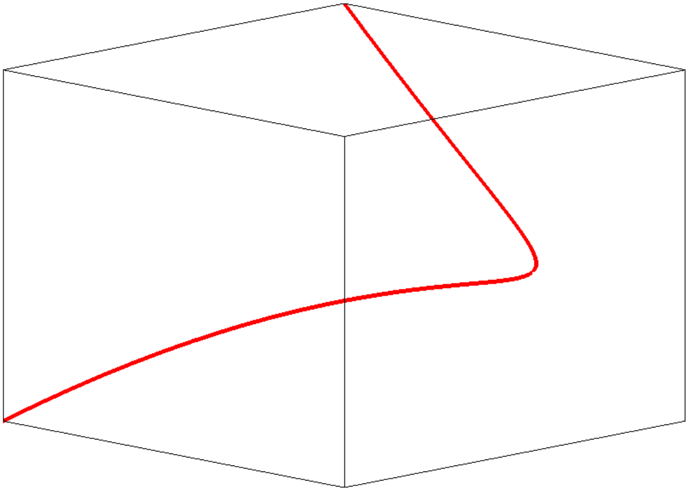


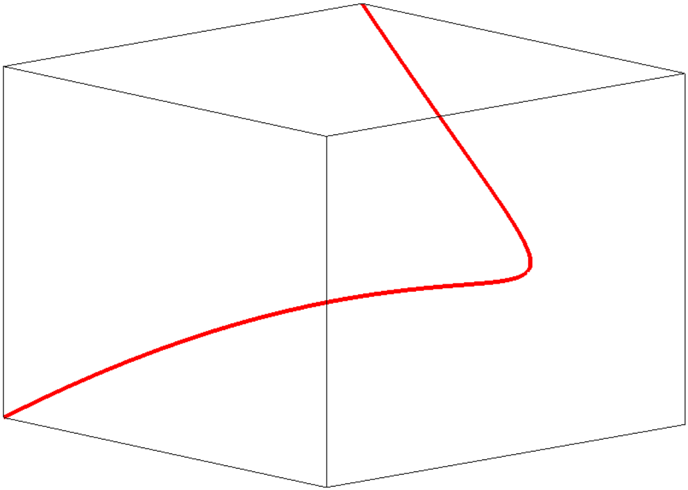


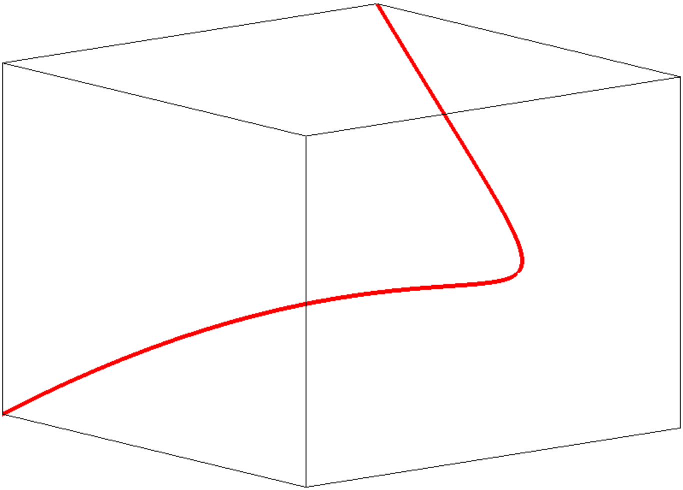


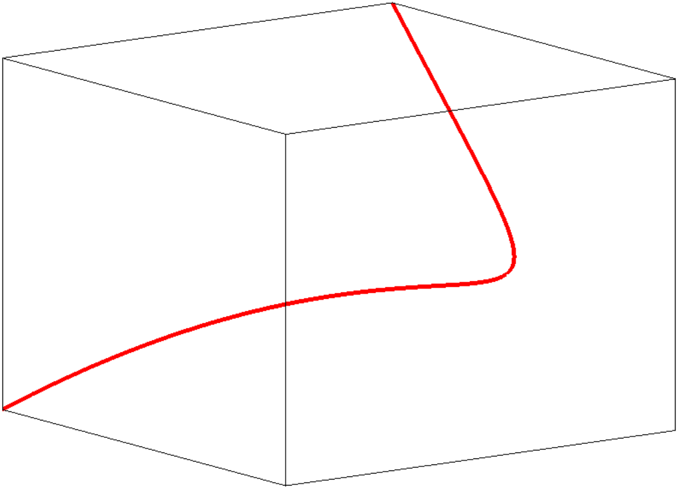


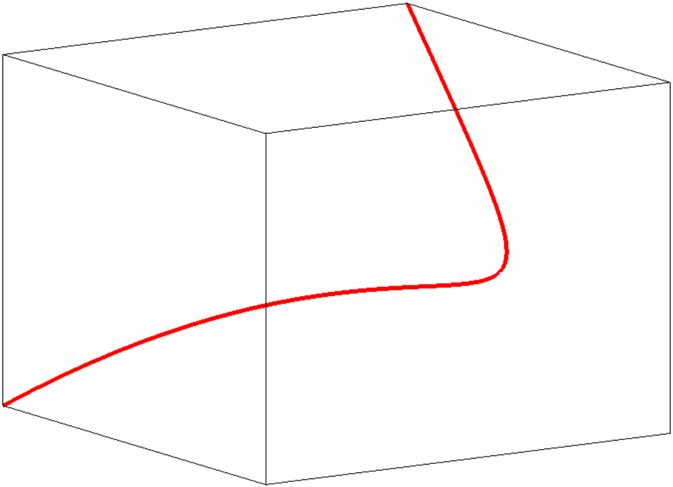


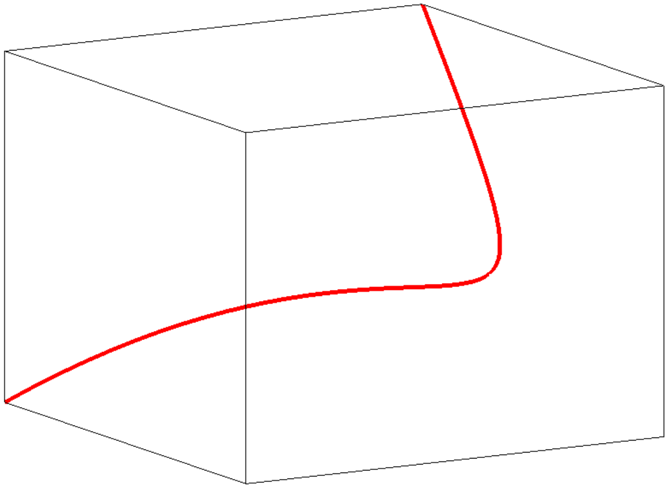


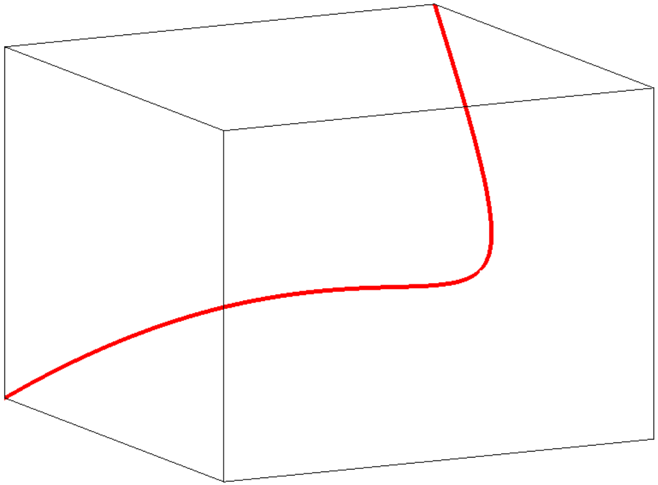


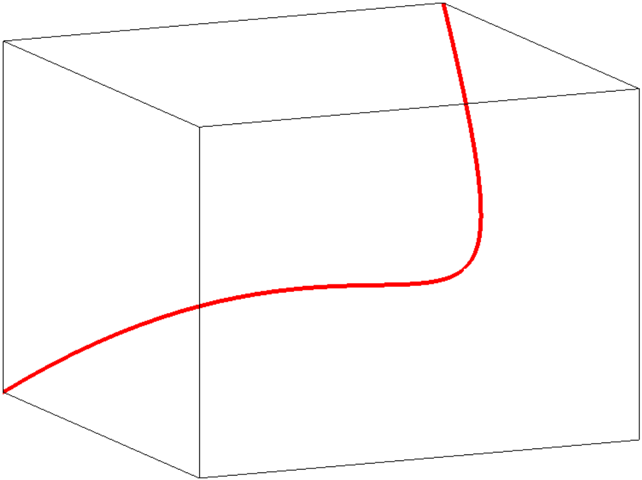


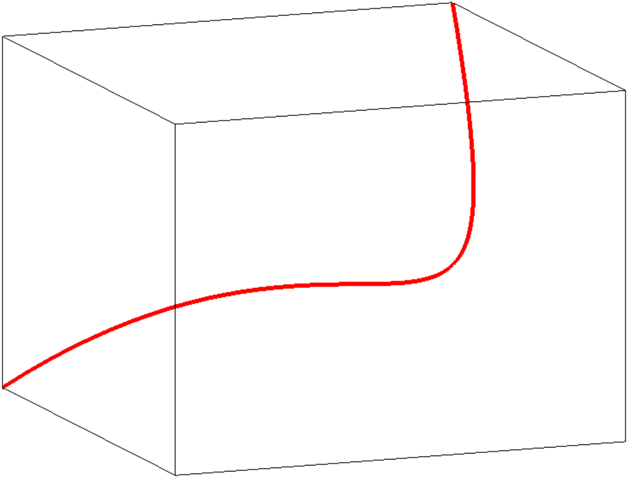


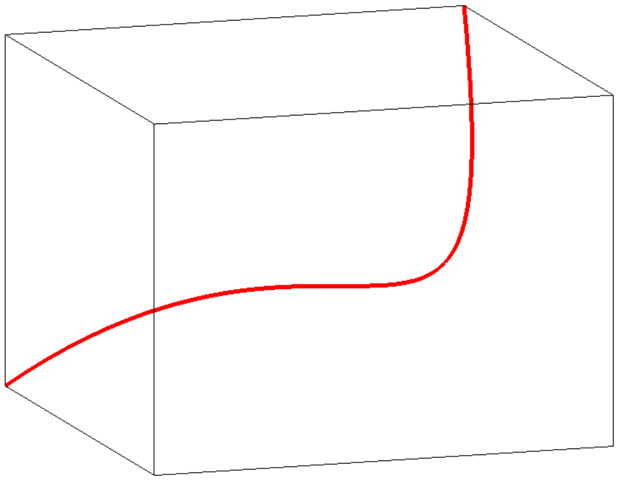


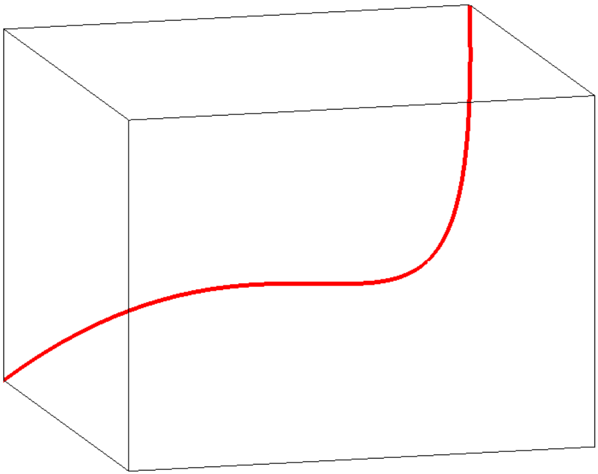


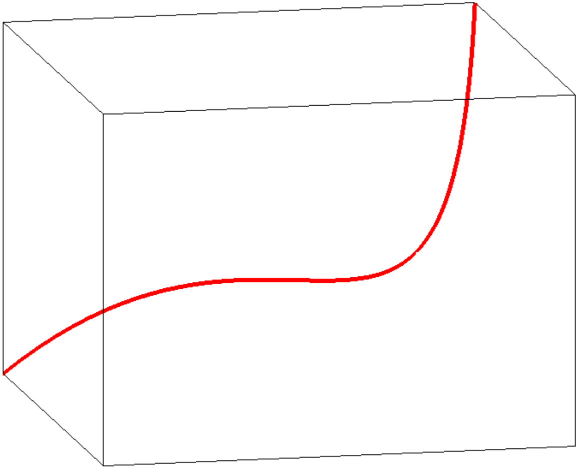


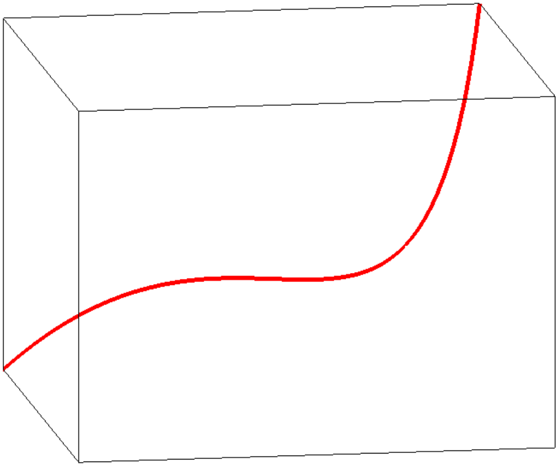


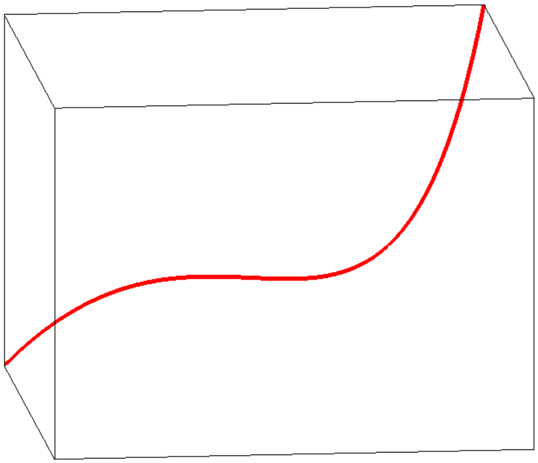


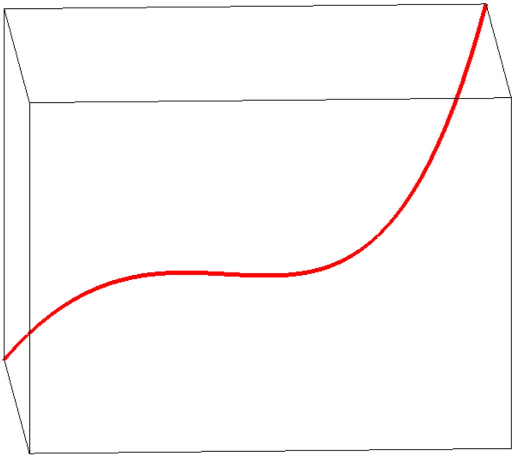


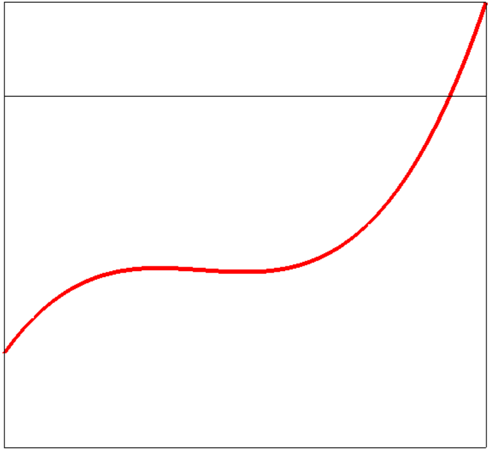


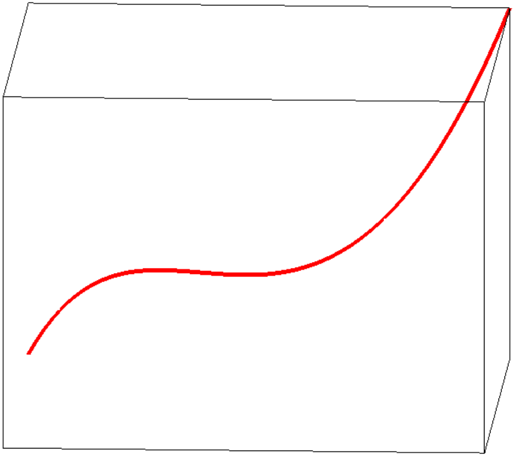


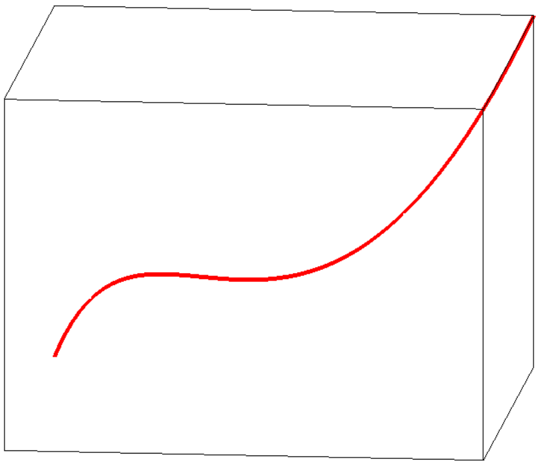


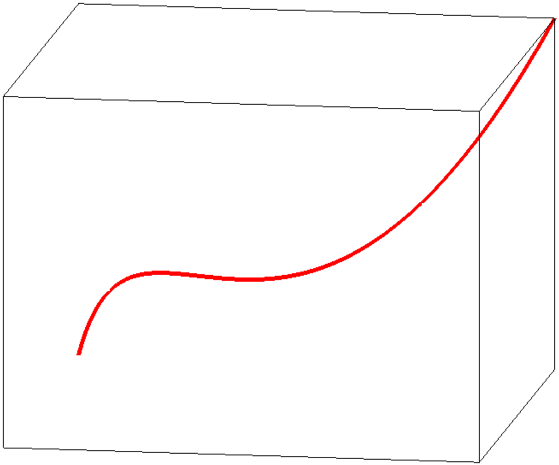


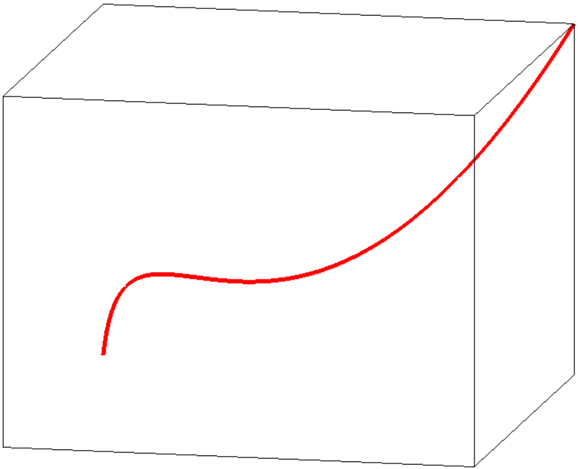


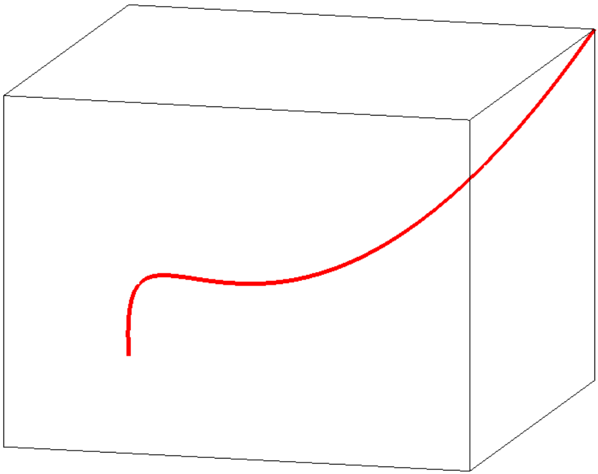


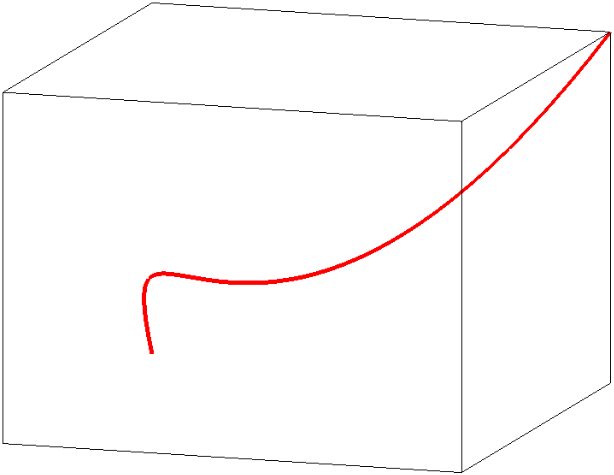


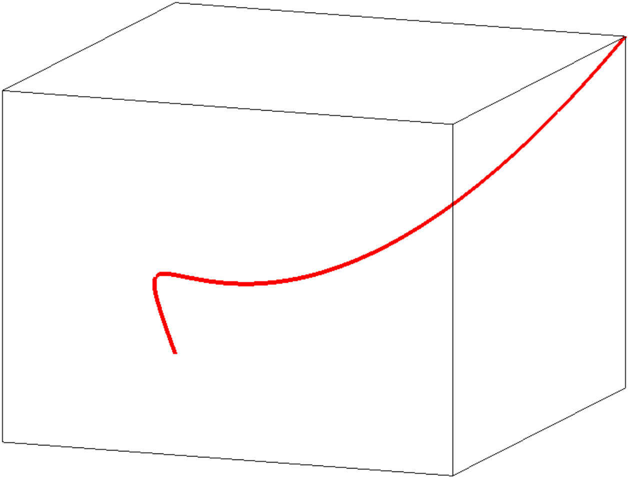


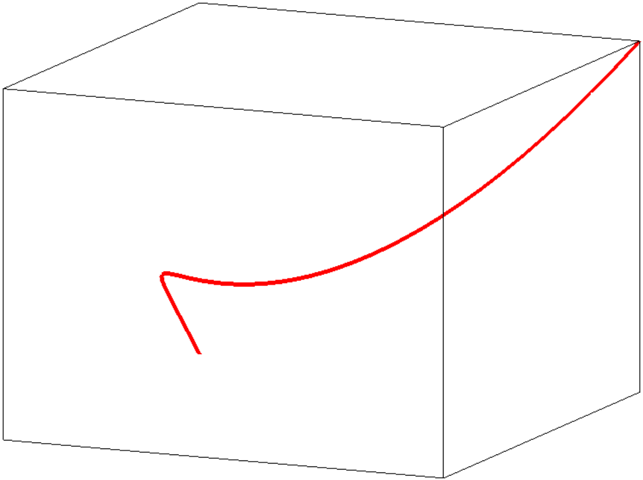


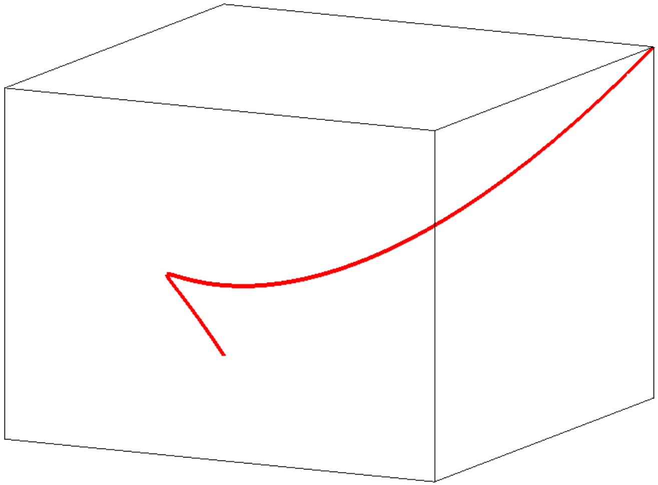


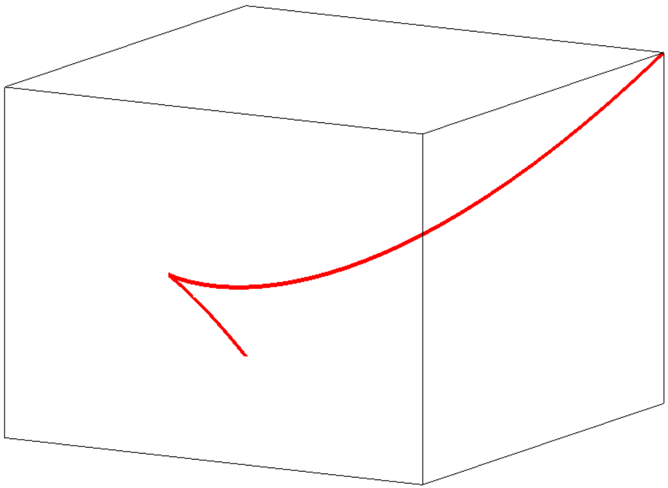


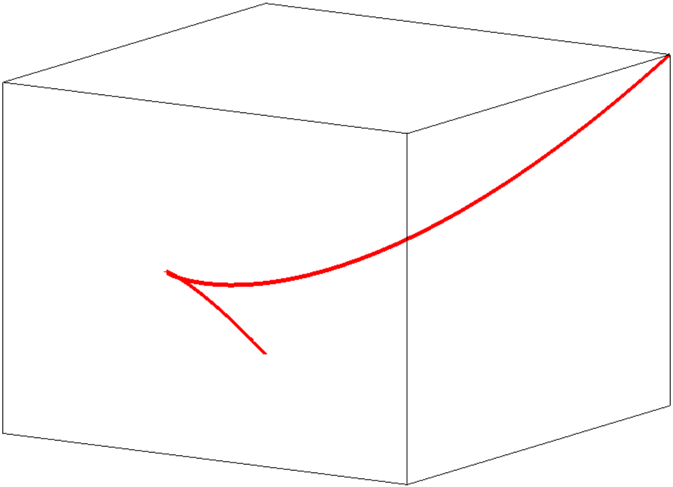


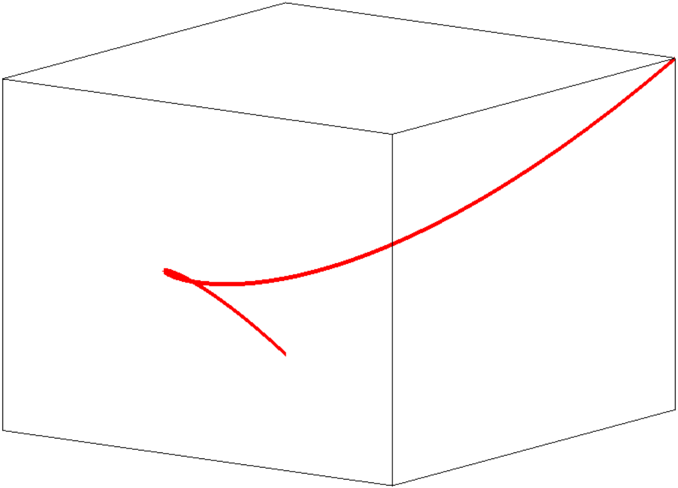


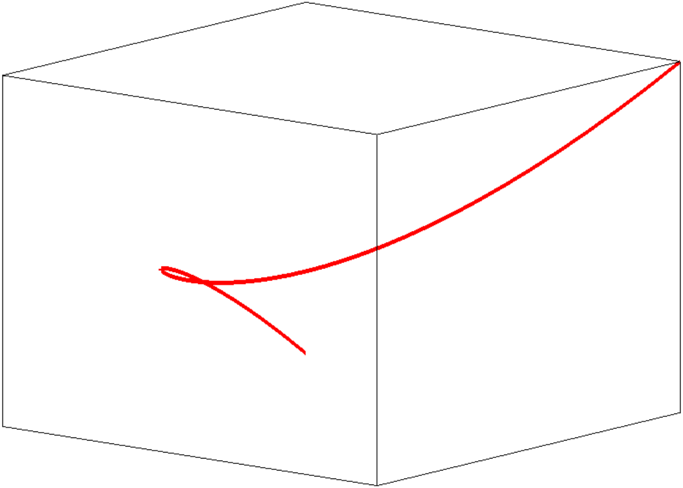


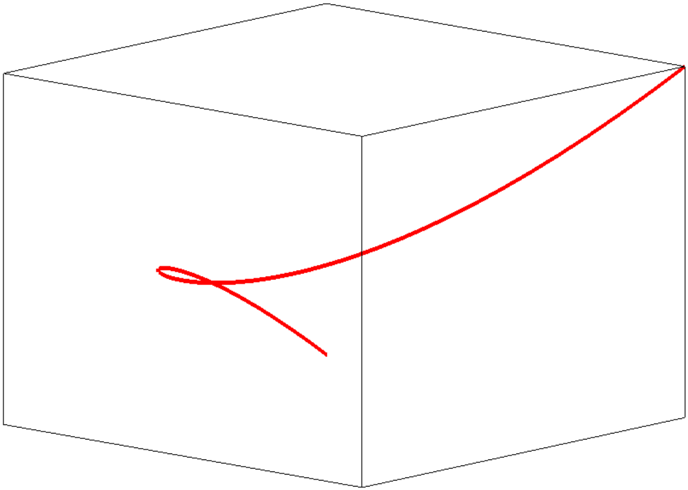


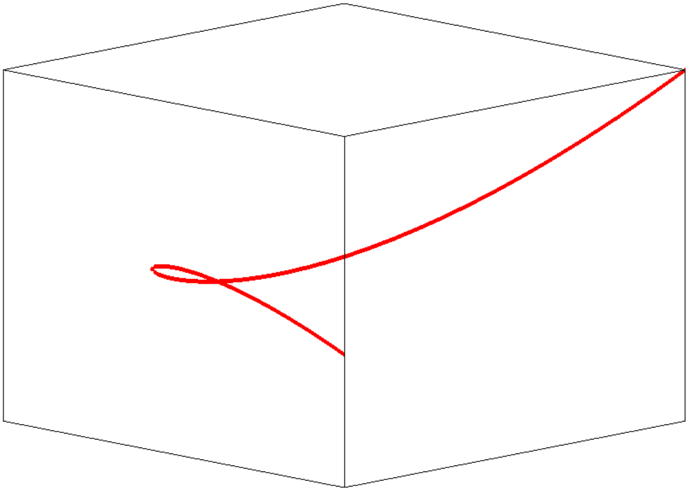


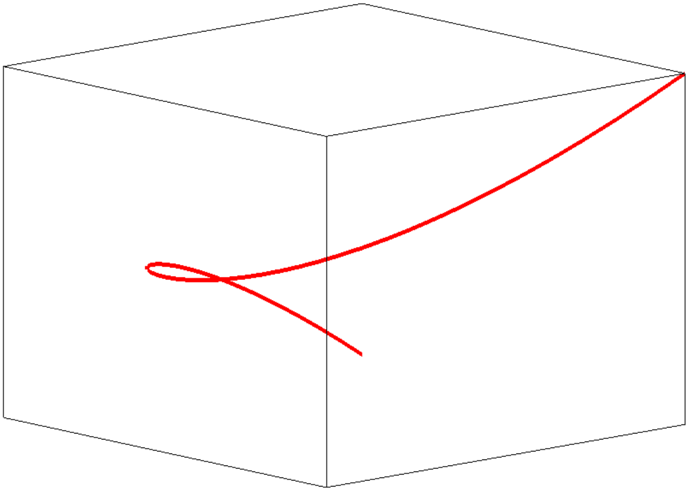


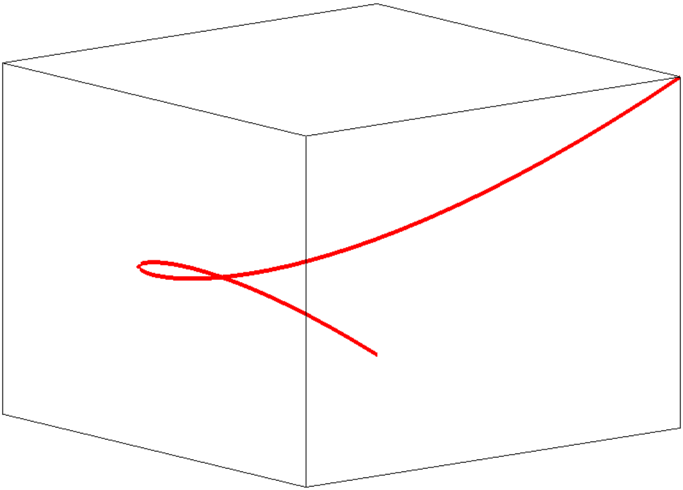


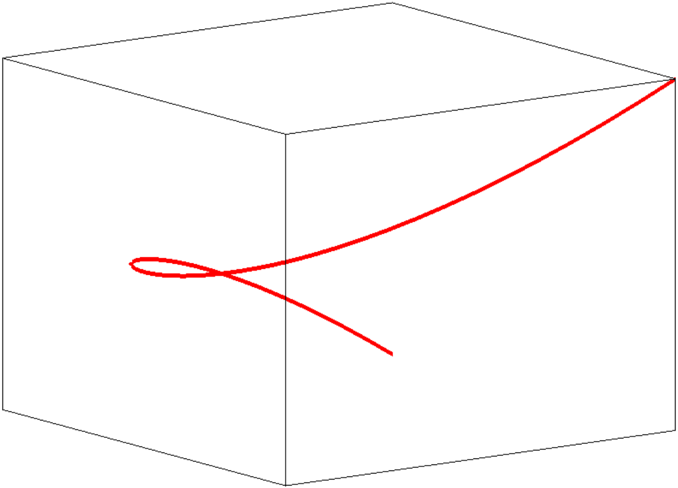


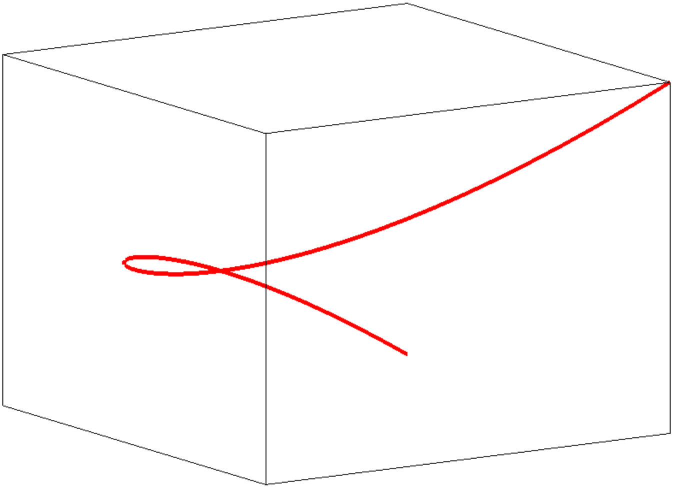


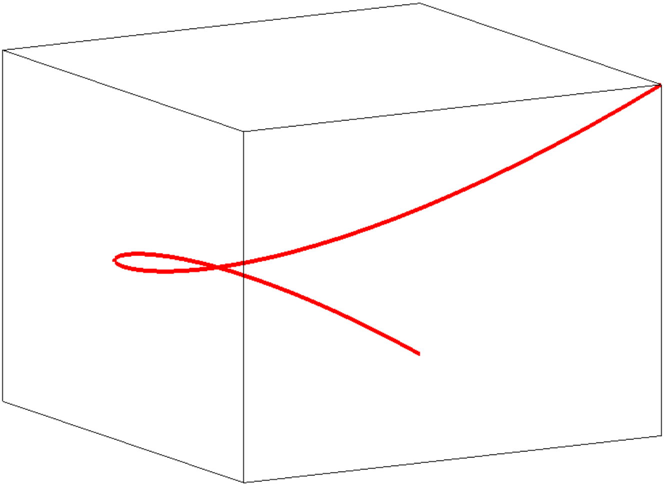


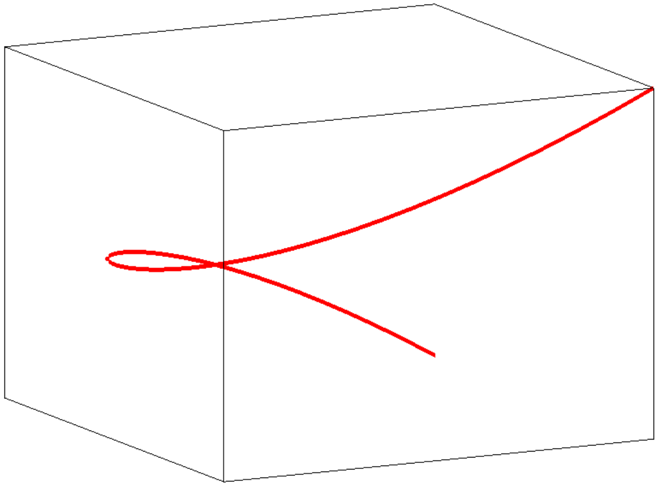


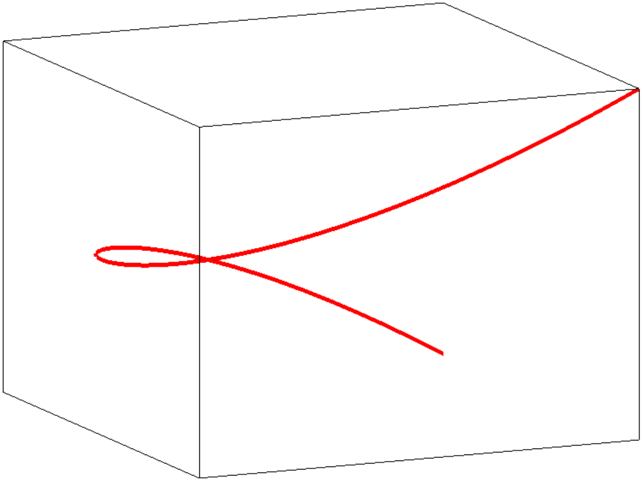


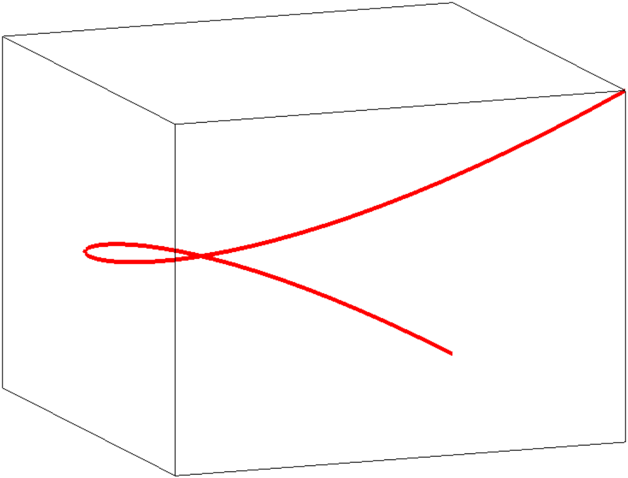


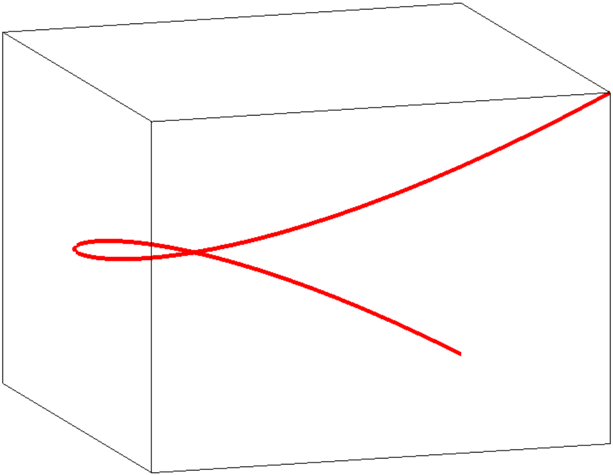


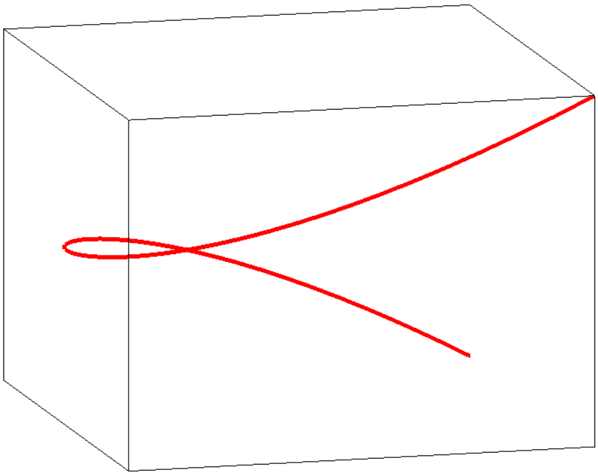


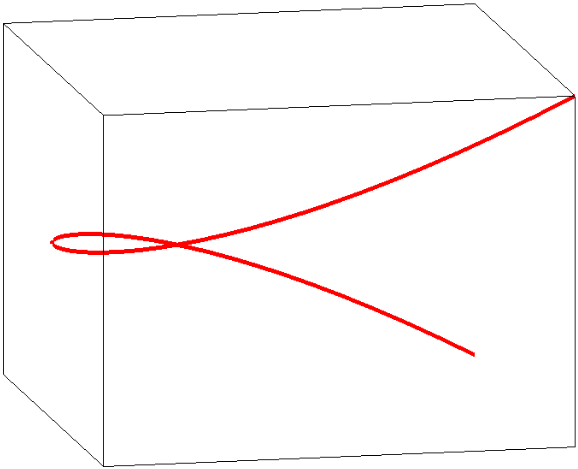


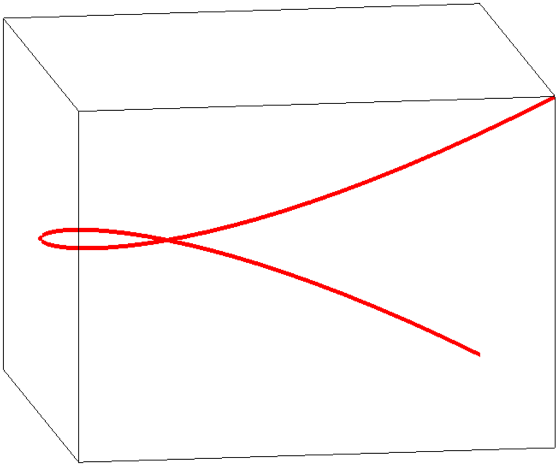


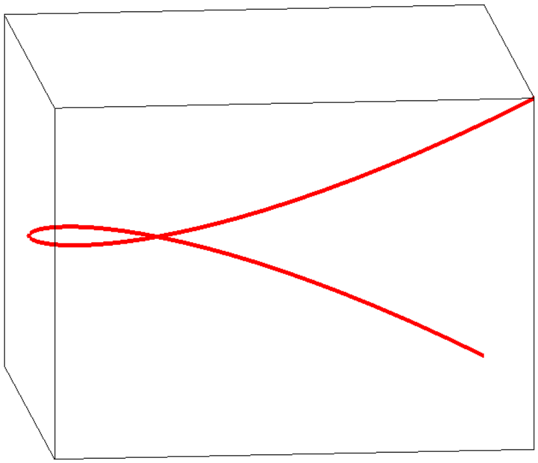


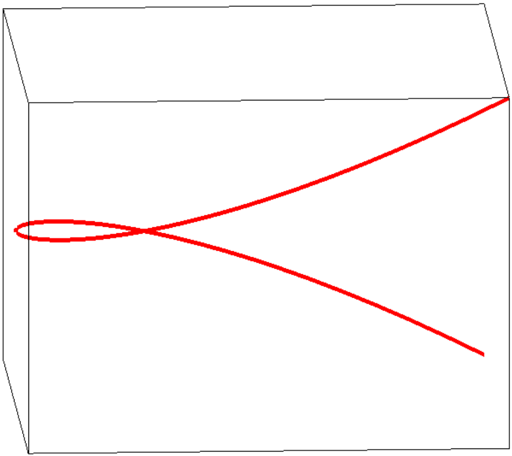


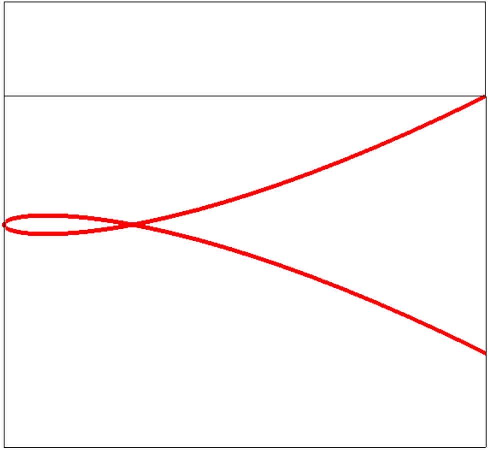












Ideals and Varieties

The affine variety $V(f_1, \ldots, f_r)$ only depends on the ideal

$$I = \langle f_1, \ldots, f_r \rangle \subset R = K[x_1, \ldots, x_n]$$

generated by the f_i: If $f_1(p) = 0, \ldots, f_r(p) = 0$, then

$$\left(\sum_{i=1}^{r} s_i \cdot f_i \right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

for all $s_i \in R$.

Ideals and Varieties

The affine variety $V(f_1, ..., f_r)$ only depends on the ideal

$$I = \langle f_1, ..., f_r \rangle \subset R = K[x_1, ..., x_n]$$

generated by the f_i: If $f_1(p) = 0, ..., f_r(p) = 0$, then

$$\left(\sum_{i=1}^{r} s_i \cdot f_i\right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

for all $s_i \in R$. Hence, we define for an ideal $I \subset R$

$$V(I) = \{p \in K^n \mid f(p) = 0 \ \forall f \in I\}$$

Ideals and Varieties

The affine variety $V(f_1, ..., f_r)$ only depends on the ideal

$$I = \langle f_1, ..., f_r \rangle \subset R = K[x_1, ..., x_n]$$

generated by the f_i: If $f_1(p) = 0, ..., f_r(p) = 0$, then

$$\left(\sum_{i=1}^{r} s_i \cdot f_i \right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

for all $s_i \in R$. Hence, we define for an ideal $I \subset R$

$$V(I) = \{ p \in K^n \mid f(p) = 0 \ \forall f \in I \}$$

This is indeed an algebraic variety: A ring is called **Noetherian** if every ideal is finitely generated.

Theorem (Hilbert's basis theorem, 1890)

If R is a Noetherian ring, then $R[x]$ is also Noetherian.

Ideals and Varieties

A variety $V(I) \subset K^n$ is called **irreducible**, if it does not have a non-trivial decomposition

$$V(I) = V(J_1) \cup V(J_2)$$

Ideals and Varieties

A variety $V(I) \subset K^n$ is called **irreducible**, if it does not have a non-trivial decomposition

$$V(I) = V(J_1) \cup V(J_2)$$

For a subset $S \subset K^n$ define the **vanishing ideal**

$$I(S) = \{f \in R \mid f(p) = 0 \; \forall p \in S\}$$

Theorem

If K is algebraically closed then

$$\{\text{prime ideals of } R\} \quad \overset{V}{\underset{I}{\rightleftarrows}} \quad \{\text{irreducible affine varieties in } K^n\}$$

is a bijection.

Projection and Elimination

Gaussian elimination parametrizes the solution set L of a linear system of equations. It computes a bijective projection $L \to K^r$. In the case of non-linear systems we can proceed in a similar way:

Projection and Elimination

Gaussian elimination parametrizes the solution set L of a linear system of equations. It computes a bijective projection $L \to K^r$. In the case of non-linear systems we can proceed in a similar way:
For an ideal $I \subset R = K[x_1, ..., x_n]$ consider the **elimination ideal**

$$I_m = I \cap K[x_{m+1}, ..., x_n]$$

and the projection

$$\begin{aligned} \pi_m : \quad & K^n \to K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

Projection and Elimination

Gaussian elimination parametrizes the solution set L of a linear system of equations. It computes a bijective projection $L \to K^r$. In the case of non-linear systems we can proceed in a similar way:
For an ideal $I \subset R = K[x_1, ..., x_n]$ consider the **elimination ideal**

$$I_m = I \cap K[x_{m+1}, ..., x_n]$$

and the projection

$$\pi_m : \quad K^n \to K^{n-m}$$
$$\pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n)$$

Theorem

$$\overline{\pi_m(V(I))} = V(I_m)$$

Projection and Elimination

Gaussian elimination parametrizes the solution set L of a linear system of equations. It computes a bijective projection $L \to K^r$. In the case of non-linear systems we can proceed in a similar way:
For an ideal $I \subset R = K[x_1, ..., x_n]$ consider the **elimination ideal**

$$I_m = I \cap K[x_{m+1}, ..., x_n]$$

and the projection

$$\begin{aligned} \pi_m : \quad & K^n \to K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

Theorem

$$\overline{\pi_m(V(I))} = V(I_m)$$

How to compute I_m?

Division with Remainder

For an ideal $I = \langle f_1, \ldots, f_r \rangle$ in the Euclidean domain (and hence PID) $K[x]$, the Euclidean algorithm computes a generator of $I = \langle \mathrm{ggT}\,(f_1, \ldots, f_r) \rangle$. Using division with remainder (successively removing the term of highest degree), we can test whether $f \in K[x]$ is in I.

Division with Remainder

For an ideal $I = \langle f_1, ..., f_r \rangle$ in the Euclidean domain (and hence PID) $K[x]$, the Euclidean algorithm computes a generator of $I = \langle \mathrm{ggT}\,(f_1, ..., f_r) \rangle$.
Using division with remainder (successively removing the term of highest degree), we can test whether $f \in K[x]$ is in I.
For $f \in R = K[x_1, ..., x_n]$ one has to choose a **lead term** $\mathrm{LT}(f)$, e.g., by ordering the terms **lexicographically** w.r.t $x_1 > ... > x_n$.

Example

We divide $x^2y + xy^2 + y^2$ by $xy - 1$ and $y^2 - 1$ for $x > y$:

$$
\begin{array}{l}
x^2y + xy^2 + y^2 = \quad x\,(xy-1) + y\,(xy-1) + x + 1\,(y^2-1) + y + 1 \\
x^2y - x \\
\hline
xy^2 + x + y^2 \\
xy^2 - y \\
\hline
x + y^2 + y \\
\hline
y^2 + y \\
y^2 - 1 \\
\hline
y + 1
\end{array}
$$

We divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot (x^2 + y) + (-y^2 - y) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

We divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$

$$\begin{array}{l} x^2 - y^2 = \quad 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y \\ \hline -y^2 - y \end{array}$$

This is strange! We have

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

hence $x^2 - y^2 \in I = \left\langle x^2 + y, xy + x \right\rangle$, but the remainder is not zero.

We divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

This is strange! We have

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

hence $x^2 - y^2 \in I = \left\langle x^2 + y, xy + x \right\rangle$, but the remainder is not zero.
Problem: Lead terms cancel.

We divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

This is strange! We have

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

hence $x^2 - y^2 \in I = \left\langle x^2 + y, xy + x \right\rangle$, but the remainder is not zero.
Problem: Lead terms cancel.
Solution: Add to the divisors all elements of I which can be obtained by cancelling lead terms and reducing by the ones we already have. This is **Buchberger's algorithm** [Buchberger, 1976], the basis of computational commutative algebra, and the result is called a **Gröbner basis** of I.

We divide $x^2 - y^2$ by $x^2 + y$ and $xy + x$

$$\begin{array}{rl} x^2 - y^2 = & 1 \cdot \left(x^2 + y\right) + \left(-y^2 - y\right) \\ x^2 + y & \\ \hline -y^2 - y & \end{array}$$

This is strange! We have

$$x^2 - y^2 = -y\left(x^2 + y\right) + x\left(xy + x\right)$$

hence $x^2 - y^2 \in I = \left\langle x^2 + y, xy + x \right\rangle$, but the remainder is not zero.
Problem: Lead terms cancel.
Solution: Add to the divisors all elements of I which can be obtained by cancelling lead terms and reducing by the ones we already have. This is **Buchberger's algorithm** [Buchberger, 1976], the basis of computational commutative algebra, and the result is called a **Gröbner basis** of I.
Gröbner basis in the example: $G = \left\{y^2 + y, x^2 + y, xy + x\right\}$

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Example

```
                        SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations          /    version 4
                                                              0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann        \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern          \
```

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Example

```
                     SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations       /    version 4
                                                           0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann    \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern       \
```

```
> ring R = 0,(x,y),lp;
```

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Example

```
                     SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations       /    version 4
                                                           0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann     \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern        \
> ring R = 0,(x,y),lp;
> ideal I = x^2 - y^2, x^2 + y;
```

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Example

```
                    SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations     /    version 4
                                                          0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann    \   Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern      \
> ring R = 0,(x,y),lp;
> ideal I = x^2 - y^2, x^2 + y;
> I = std(I);
> I;
  _[1] = y2+y
  _[2] = xy+x
  _[3] = x2+y
```

Gröbner Bases and Ideal Membership in Singular

Theorem

If G is a Gröbner basis of $I \subset R$ and $f \in R$, then $f \in I$ iff $\mathrm{NF}(f, G) = 0$.

Example

```
                      SINGULAR                               /   Development
 A Computer Algebra System for Polynomial Computations      /    version 4
                                                          0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann   \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern      \
> ring R = 0,(x,y),lp;
> ideal I = x^2 - y^2, x^2 + y;
> I = std(I);
> I;
  _[1] = y2+y
  _[2] = xy+x
  _[3] = x2+y
> NF(x^2-y^2,I);
  0
```

Gröbner Bases and Projection

Theorem

If $G = \{g_1, \dots, g_r\}$ *is a lexicographical Gröbner basis of* $I \subset K[x_1, \dots, x_n]$, *then*

$$G_m = G \cap K[x_{m+1}, \dots, x_n]$$

is a lexicographical Gröbner basis of $I_m \subset K[x_{m+1}, \dots, x_n]$.

Theorem

If $G = \{g_1, \dots, g_r\}$ *is a lexicographical Gröbner basis of* $I \subset K[x_1, \dots, x_n]$, *then*

$$G_m = G \cap K[x_{m+1}, \dots, x_n]$$

is a lexicographical Gröbner basis of $I_m \subset K[x_{m+1}, \dots, x_n]$.

Using projections, we can compute the image of $V(I)$ under a rational map $\varphi = (\varphi_1, \dots, \varphi_r)$ with $\varphi_i \in K(x_1, \dots, x_n)$ by projecting the graph

$$\begin{array}{ccccc} & & \Gamma(\varphi) & & \\ & \swarrow^{\pi_1} & & \searrow^{\pi_2} & \\ V(I) & & \dashrightarrow & & K^r \end{array} \qquad = \{(x, \varphi(x)) \mid x \in V(I)\} \subset K^n \times K^r$$

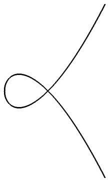
Desingularization of Curves

Given a singular curve, find smooth curve C' which is birational to C.

Desingularization of Curves

Given a singular curve, find smooth curve C' which is birational to C.

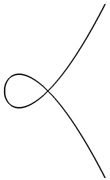
$$C = V(x^3 + x^2 - y^2)$$



Desingularization of Curves

Given a singular curve, find smooth curve C' which is birational to C.

$$C = V(x^3 + x^2 - y^2)$$



The **coordinate ring** of C (i.e. ring of functions on C) is the quotient ring

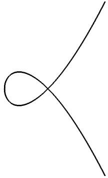
$$A = K[x, y]/I \quad \text{where} \quad I = \left\langle x^3 + x^2 - y^2 \right\rangle .$$

Suppose C' is another affine variety with coordinate ring A'.

Desingularization of Curves

Given a singular curve, find smooth curve C' which is birational to C.

$$C = V(x^3 + x^2 - y^2)$$



The **coordinate ring** of C (i.e. ring of functions on C) is the quotient ring

$$A = K[x,y]/I \quad \text{where} \quad I = \left\langle x^3 + x^2 - y^2 \right\rangle .$$

Suppose C' is another affine variety with coordinate ring A'.

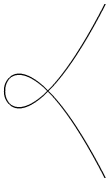
Definition

C and C' are called **birational** if $Q(A) \cong Q(A')$.

Desingularization of Curves

Given a singular curve, find smooth curve C' which is birational to C.

$$C = V(x^3 + x^2 - y^2)$$



The **coordinate ring** of C (i.e. ring of functions on C) is the quotient ring

$$A = K[x, y]/I \quad \text{where} \quad I = \langle x^3 + x^2 - y^2 \rangle .$$

Suppose C' is another affine variety with coordinate ring A'.

Definition

C and C' are called **birational** if $Q(A) \cong Q(A')$.

Equivalently: There is a rational map $C \dashrightarrow C'$ defined on a Zariski open subset of C which admits an inverse rational map.

Desingularization of Curves

Example

$$C = V(x^3 + x^2 - y^2) \xrightarrow{\varphi} K^1,\ (x,y) \longmapsto t = \frac{y}{x}$$

$$I(\Gamma(\varphi)) = \langle x^3 + x^2 - y^2,\ x \cdot t - y,\ \overbrace{w \cdot x - 1}^{\Rightarrow x \neq 0} \rangle \subset K[w,x,y,t]$$

Desingularization of Curves

Example

$$C = V(x^3 + x^2 - y^2) \xrightarrow{\varphi} K^1, \ (x, y) \longmapsto t = \frac{y}{x}$$

$$I(\Gamma(\varphi)) = \langle x^3 + x^2 - y^2, \ x \cdot t - y, \ \overset{\Rightarrow x \neq 0}{w \cdot x - 1} \rangle \subset K[w, x, y, t]$$

Elimination with $w > x > y > t$:

$x^3 + x^2 - y^2$		w		
$xt - y$	$-w$		wy	$-wt$
$wx - 1$	t	$x^2 - x$		1
$-wy + t$	1		xt	t
$-wy^2 + x^2 + x$		1	-1	
$-x^2 + xt^2 - x$			1	w
$-x + t^2 - 1$				1
$\vdots$				

Desingularization of Curves

Example

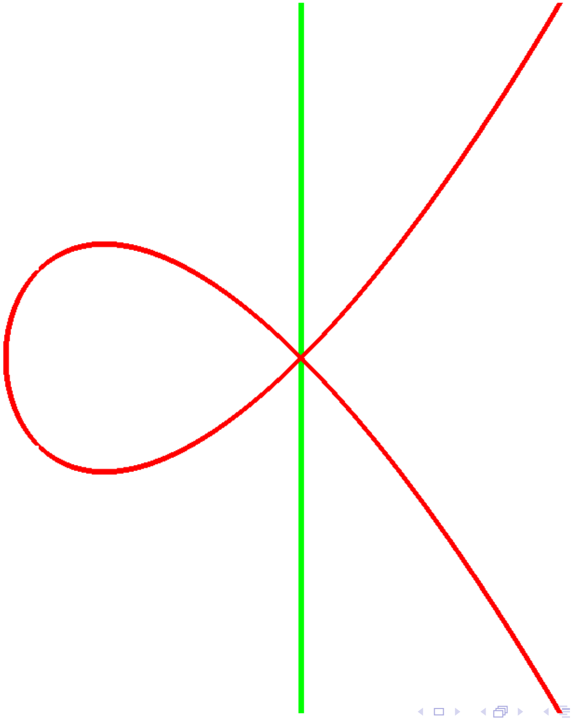
$$C = V(x^3 + x^2 - y^2) \xrightarrow{\varphi} K^1,\ (x, y) \longmapsto t = \frac{y}{x}$$

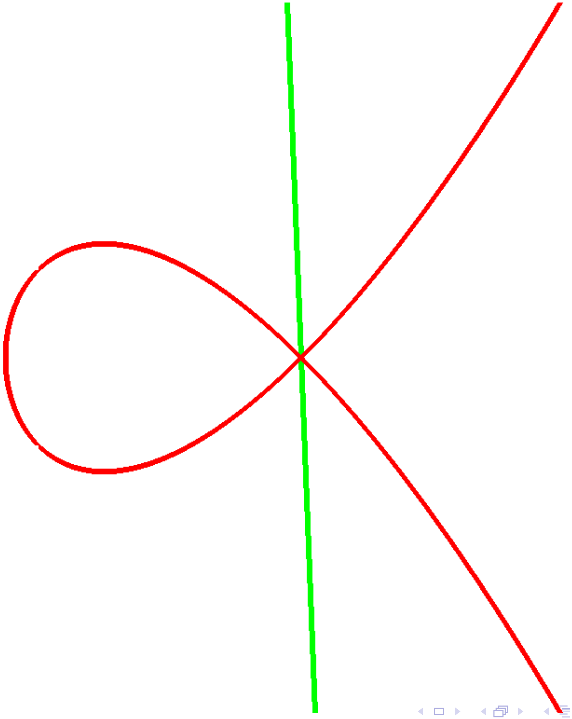
$$I(\Gamma(\varphi)) = \langle x^3 + x^2 - y^2,\ x \cdot t - y,\ \overset{\Rightarrow x \neq 0}{w \cdot x - 1} \rangle \subset K[w, x, y, t]$$

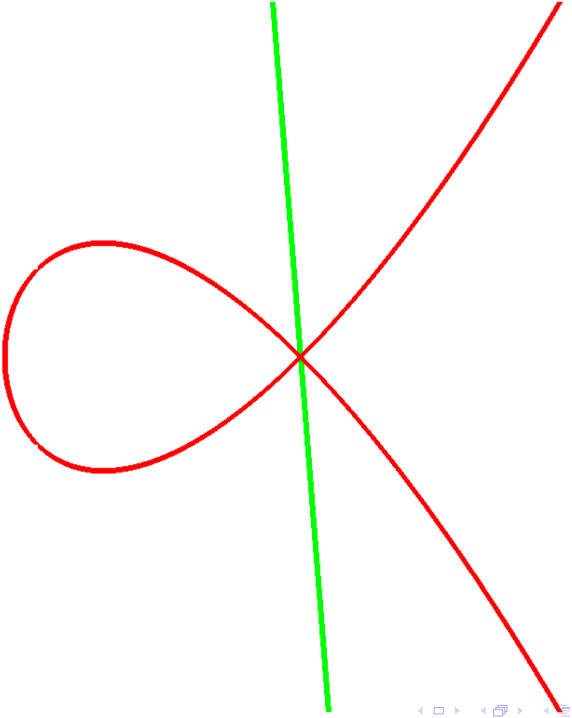
Elimination with $w > x > y > t$:

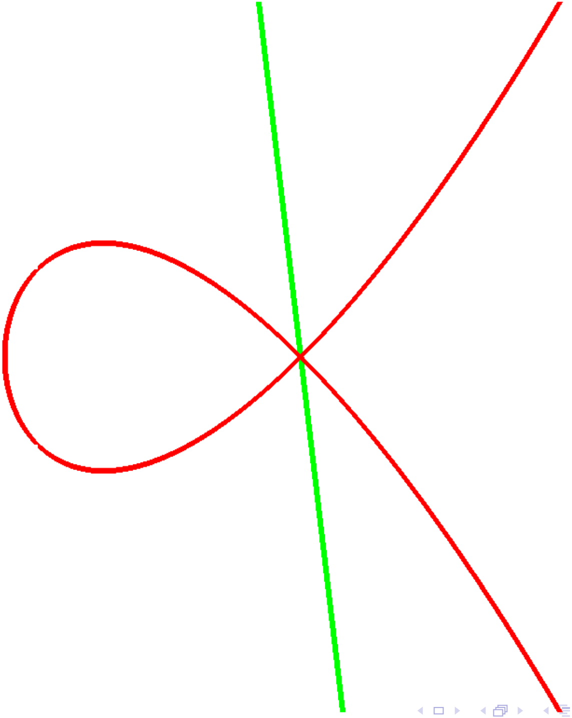
$x^3 + x^2 - y^2$		w		
$xt - y$	$-w$		wy	$-wt$
$wx - 1$	t	$x^2 - x$		1
$-wy + t$	1		xt	t
$-wy^2 + x^2 + x$		1	-1	
$-x^2 + xt^2 - x$			1	w
$-x + t^2 - 1$				1
$\vdots$				

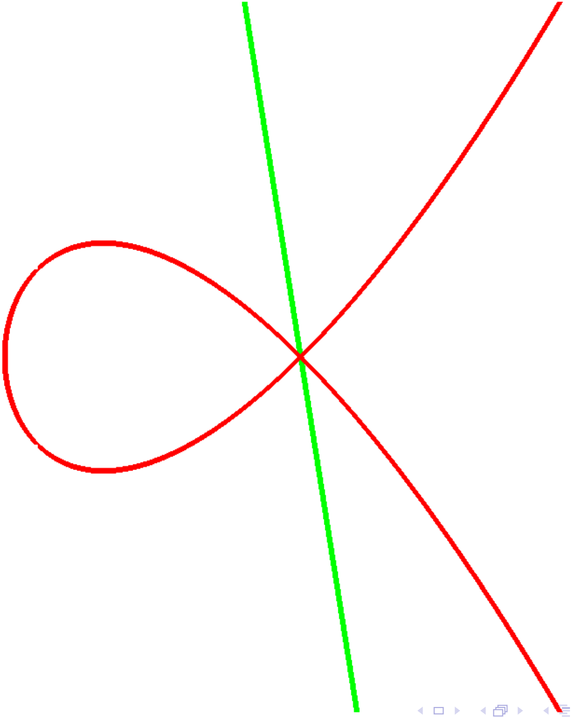
$$K^1 \xrightarrow{\varphi^{-1}} C$$
$$t \longmapsto (t^2 - 1, t^3 - t)$$

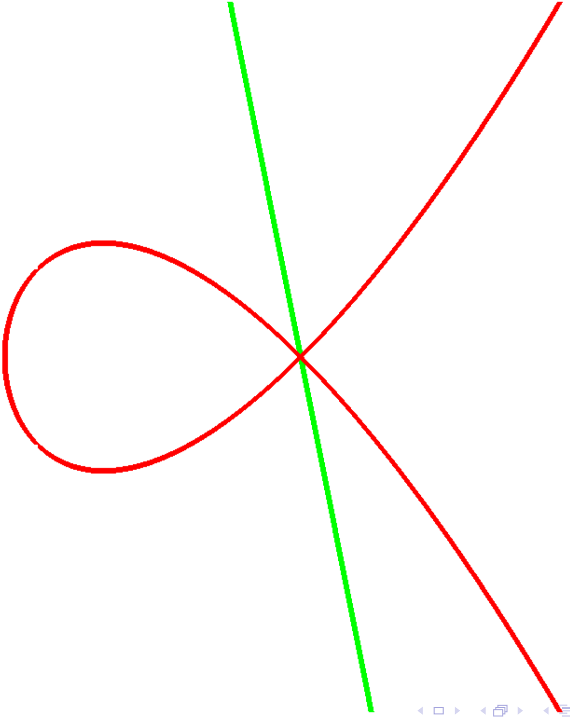


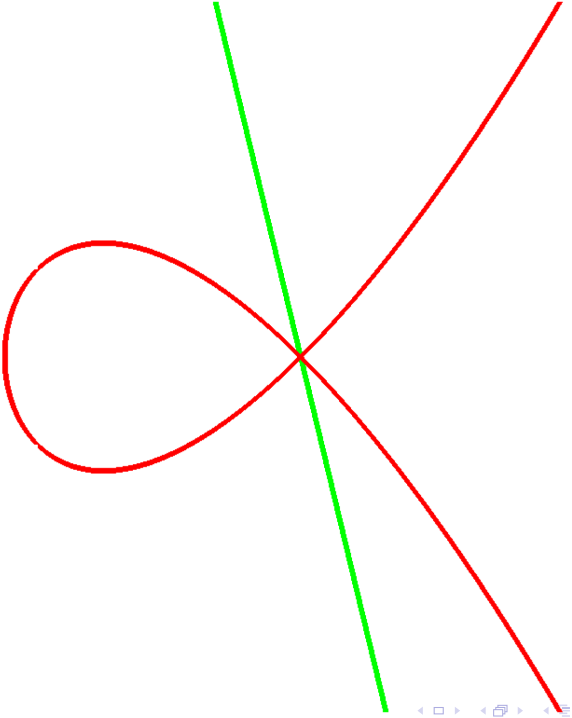


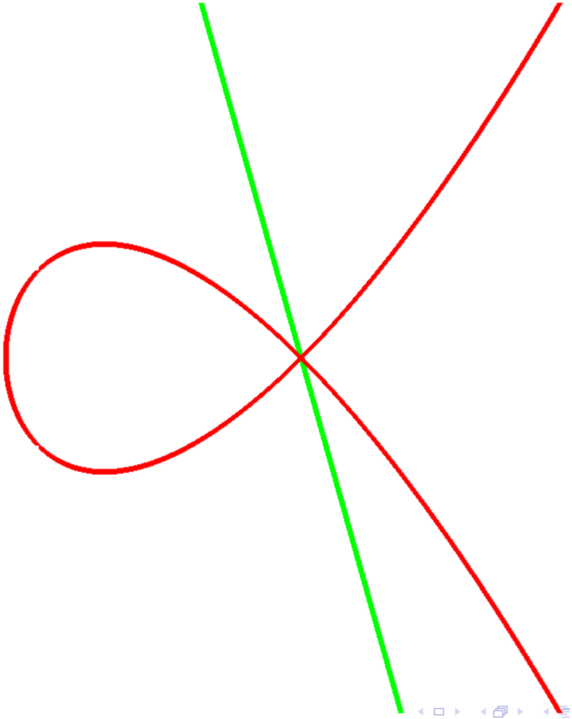


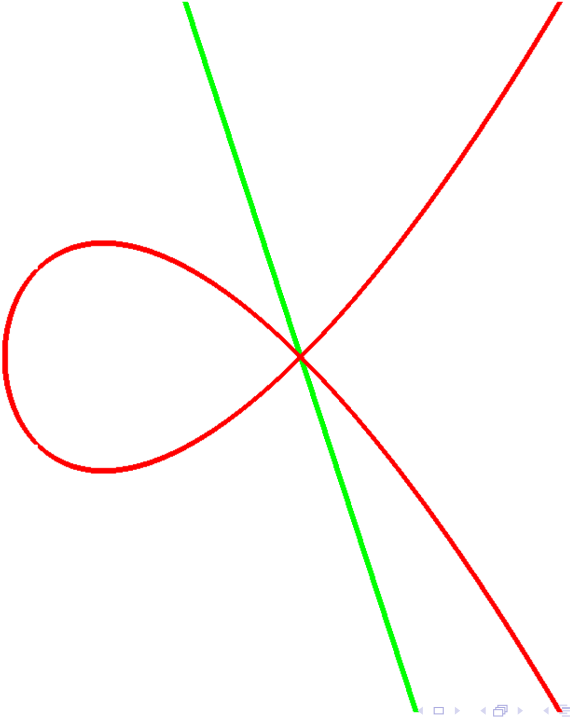


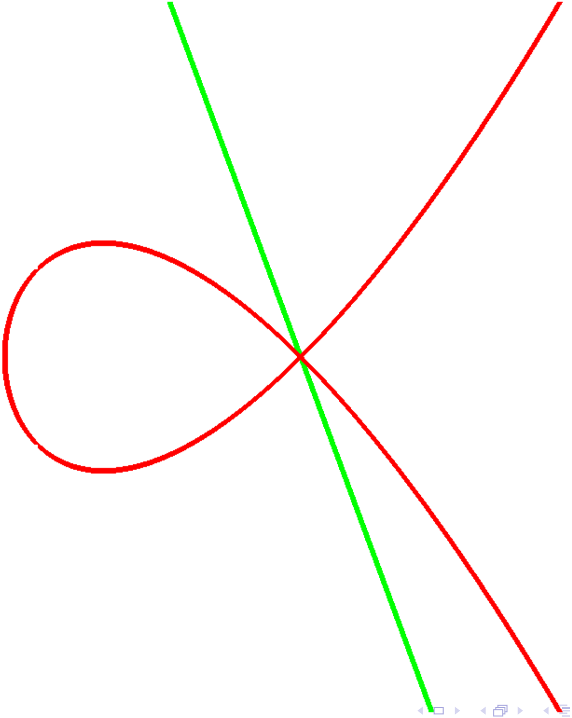


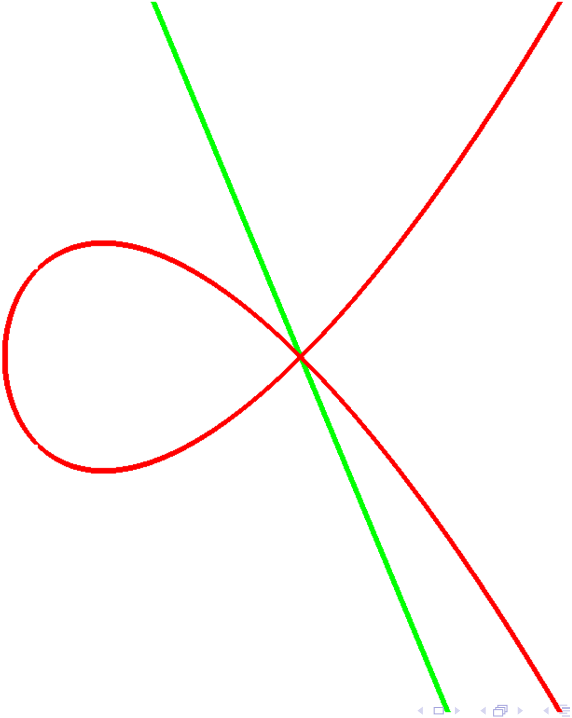


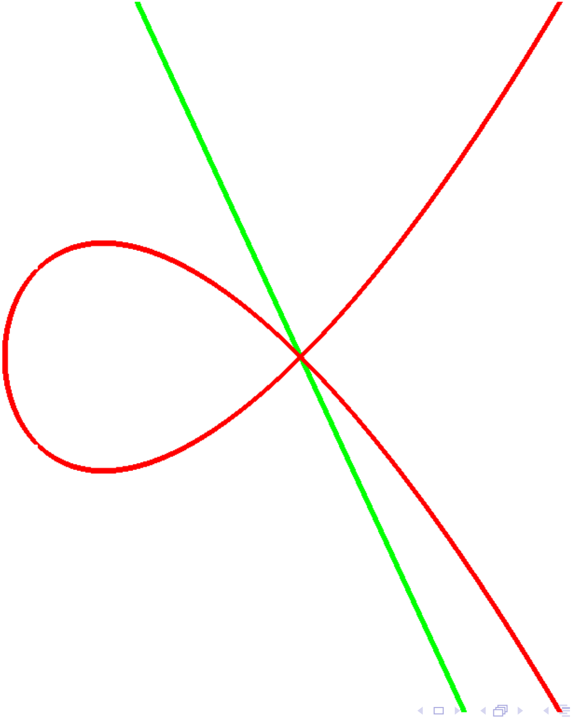


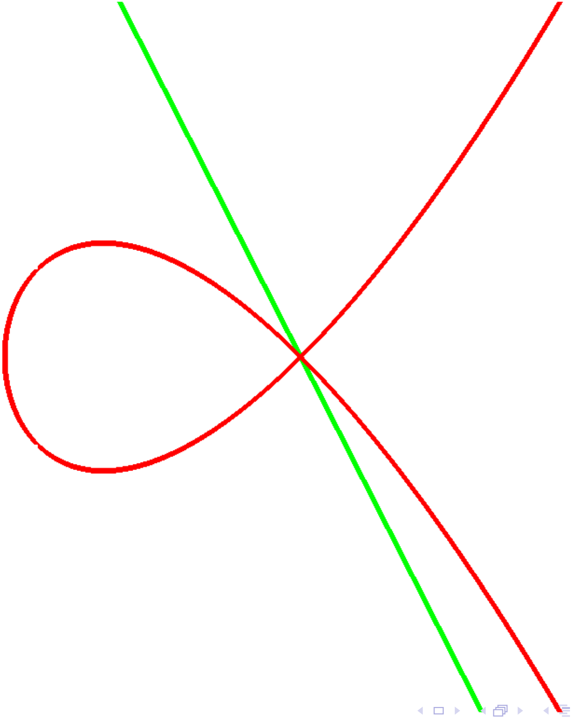


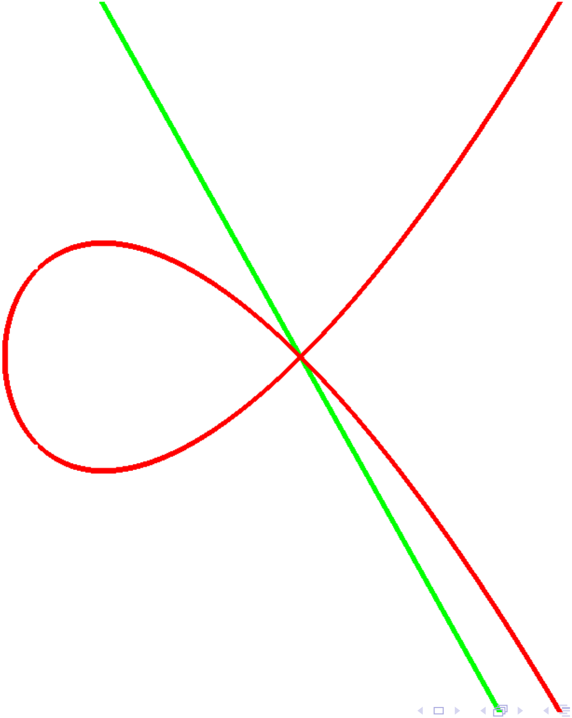


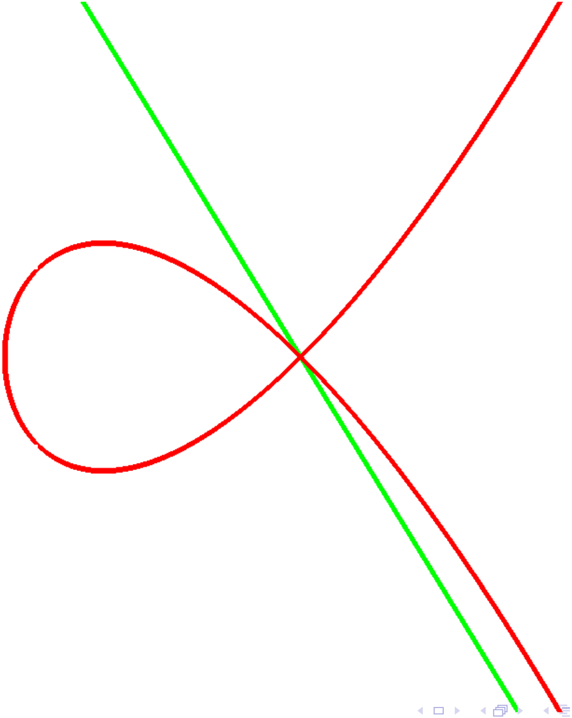


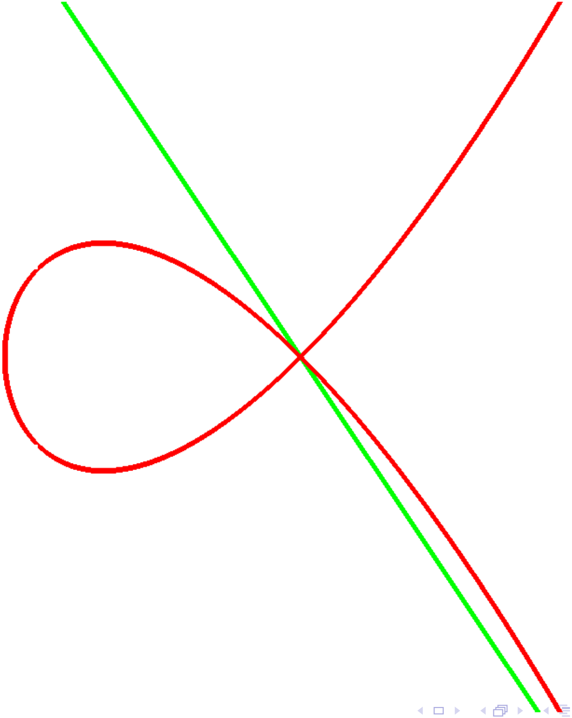


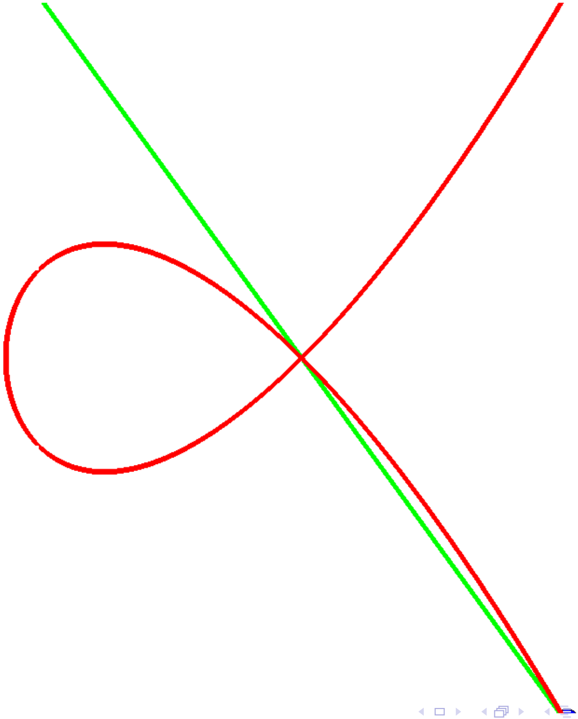


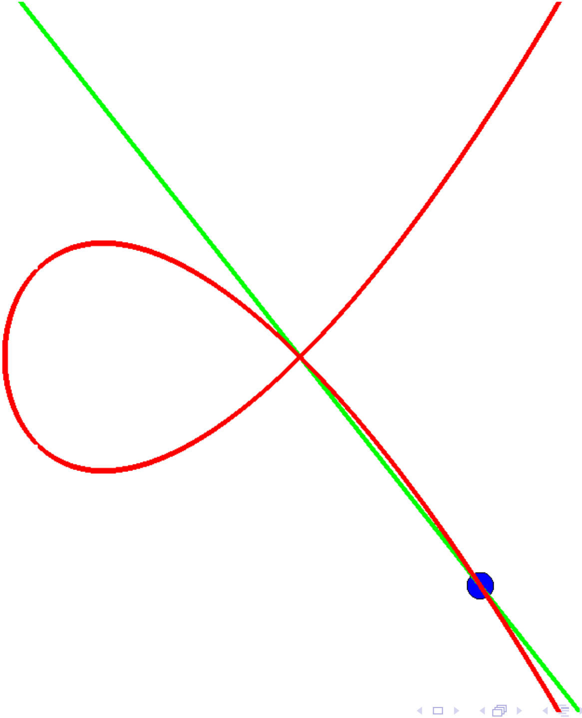


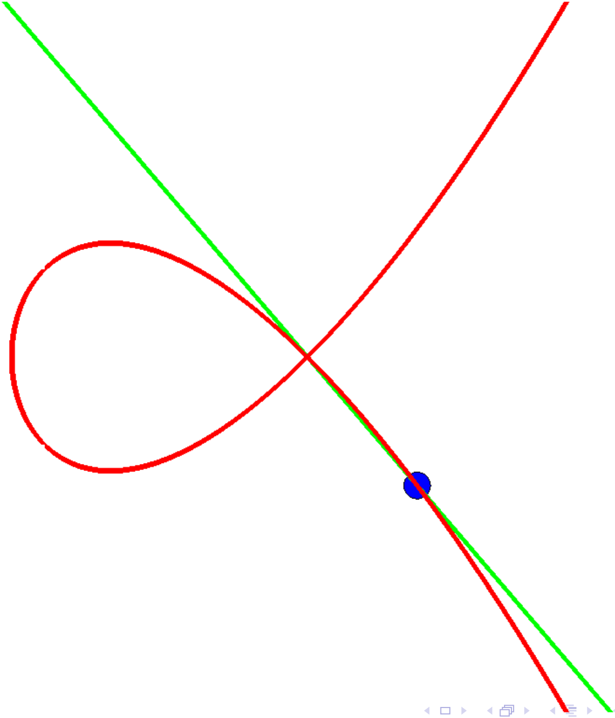


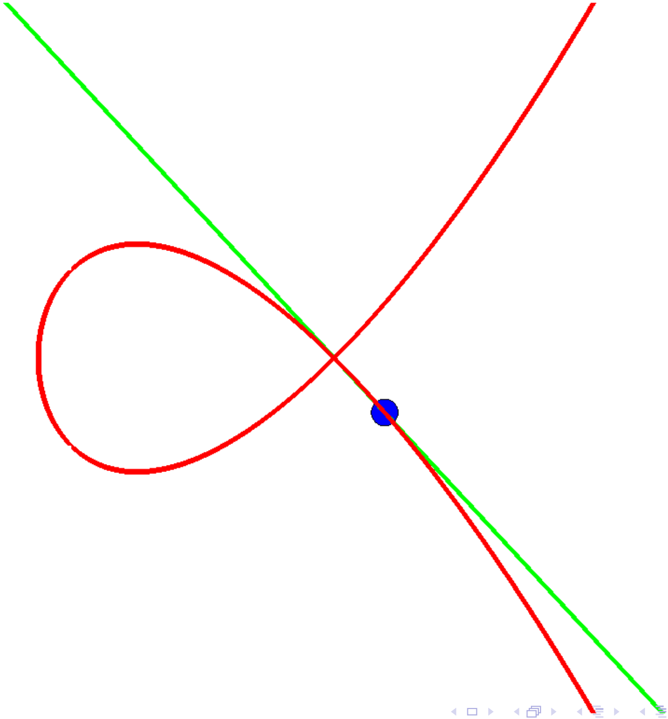


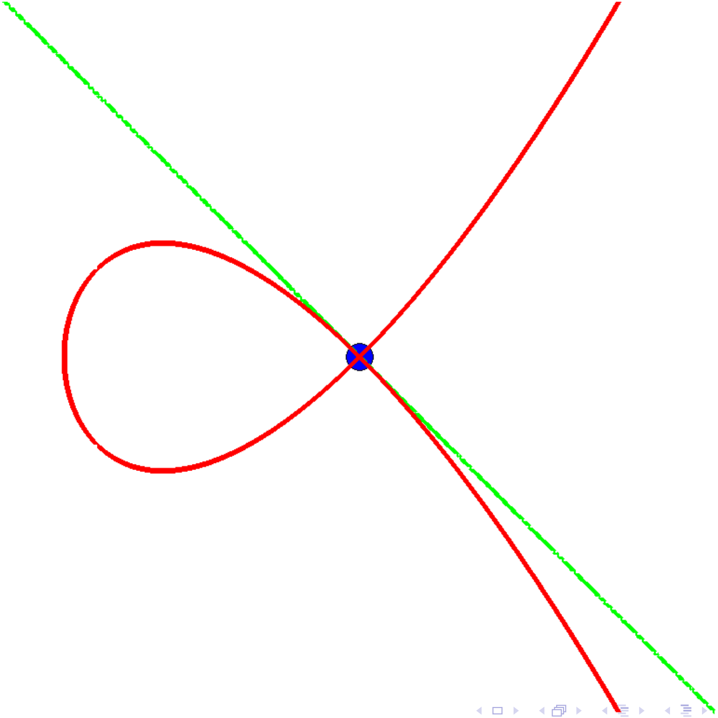


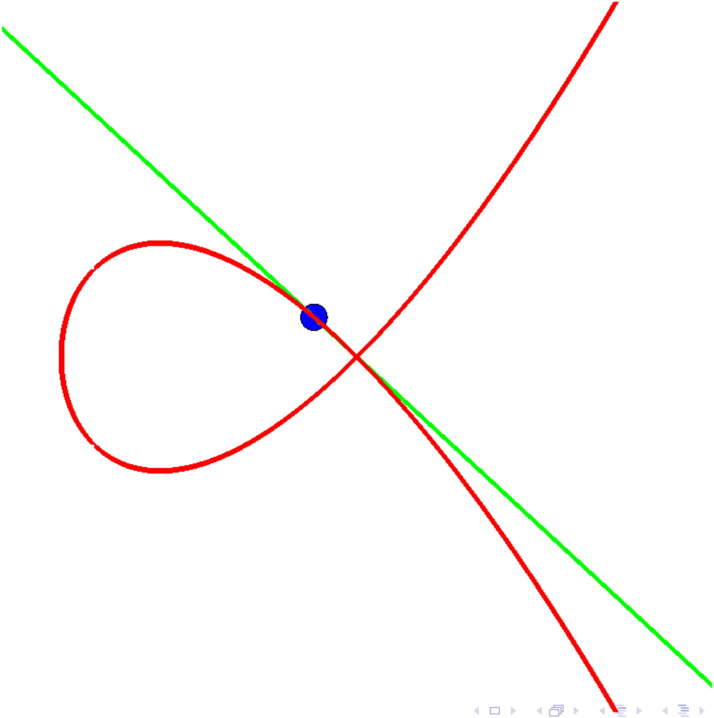


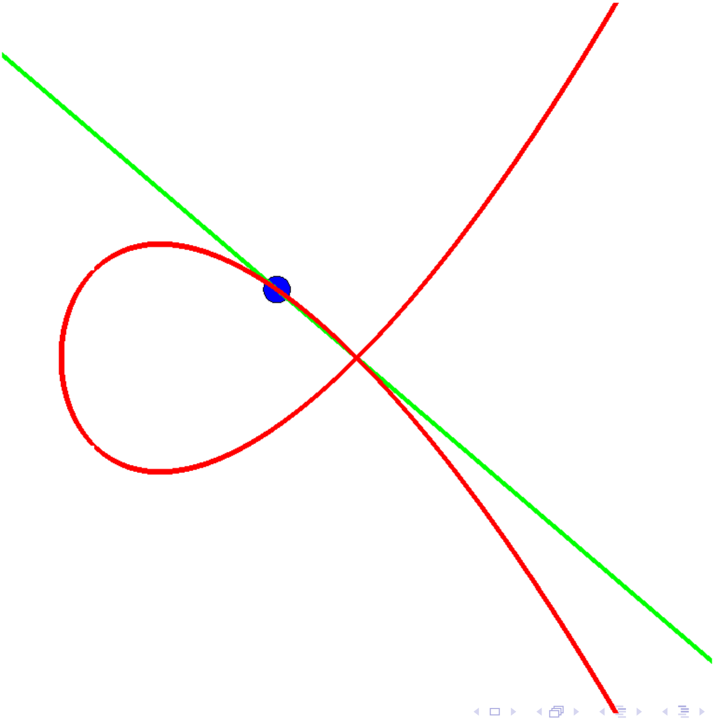


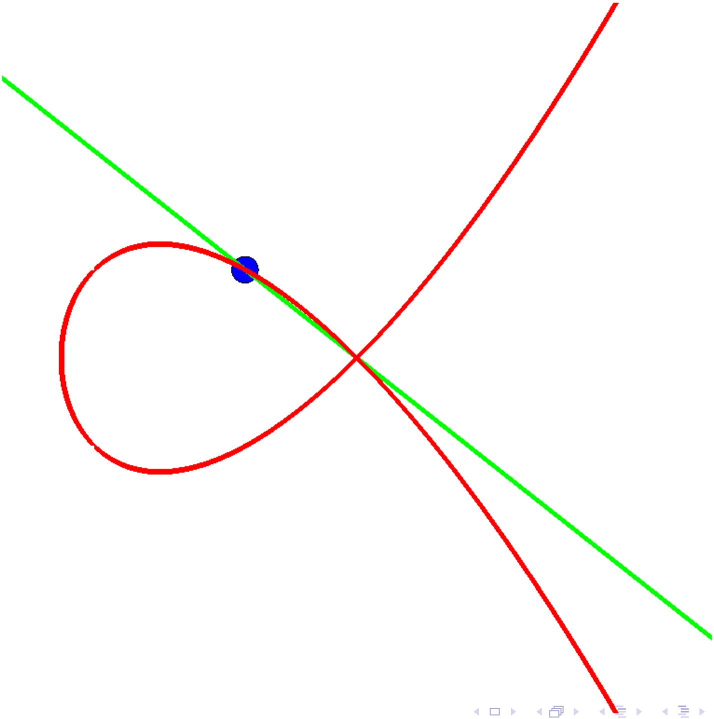


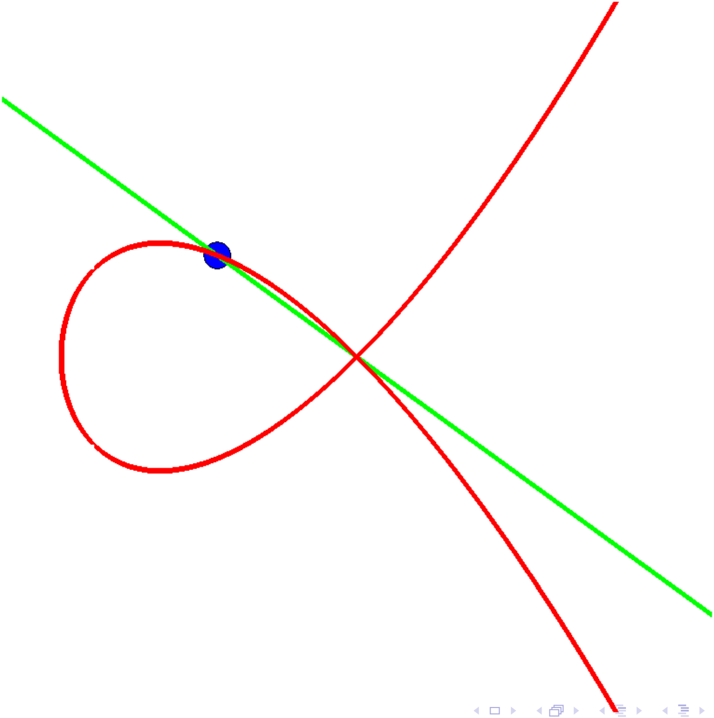


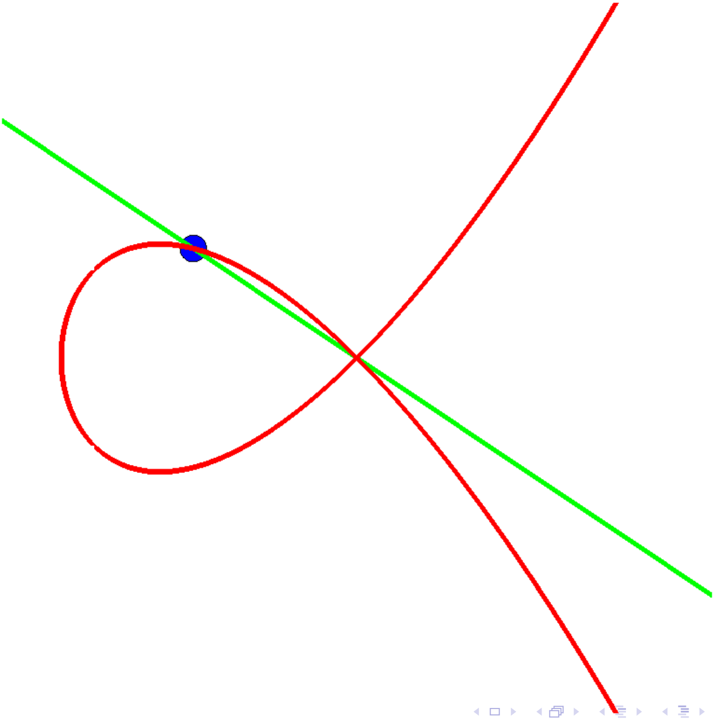


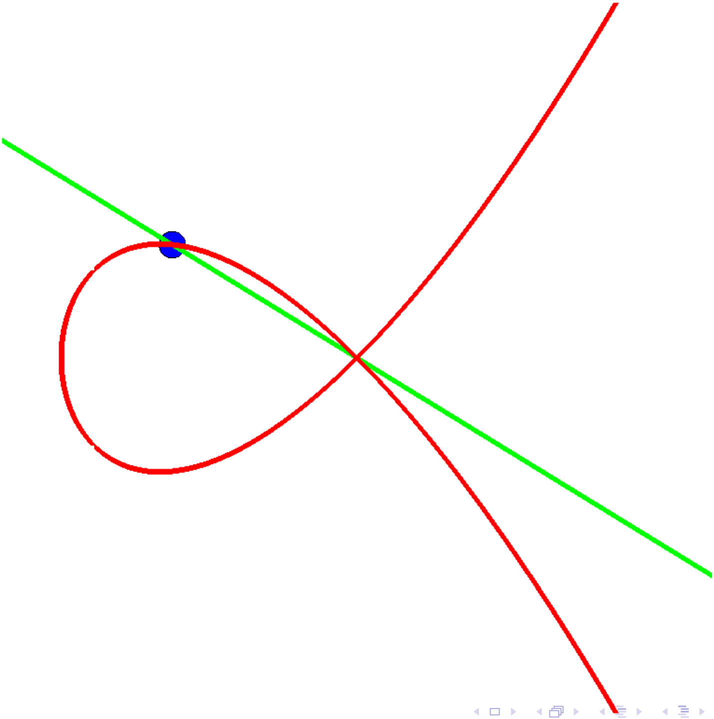


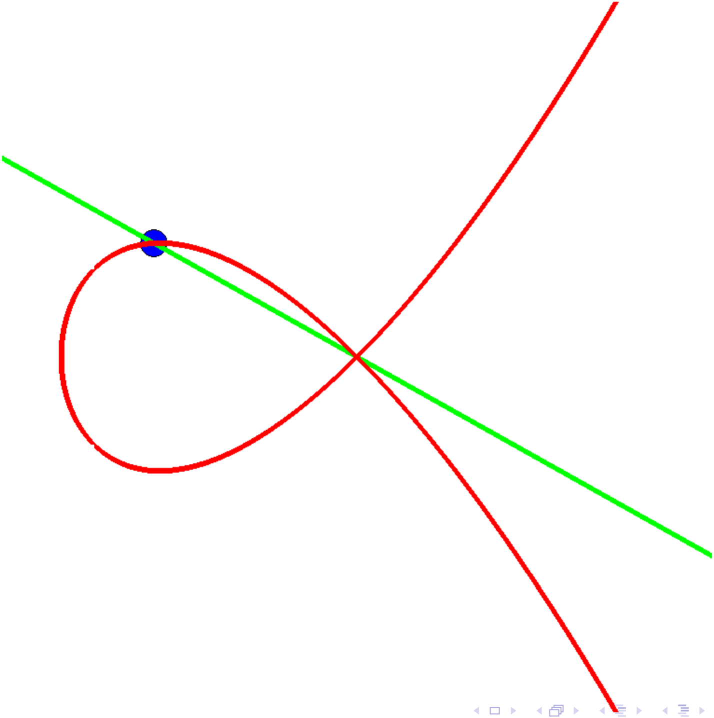


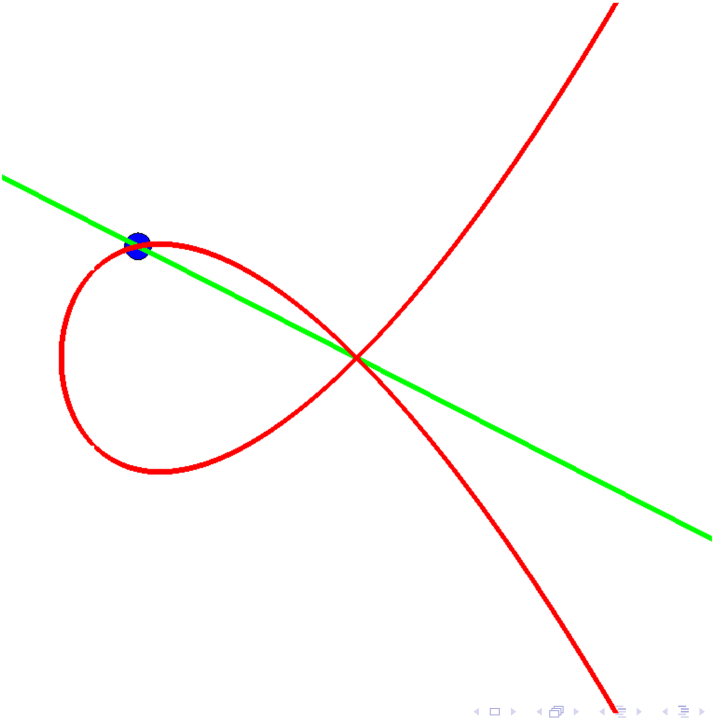


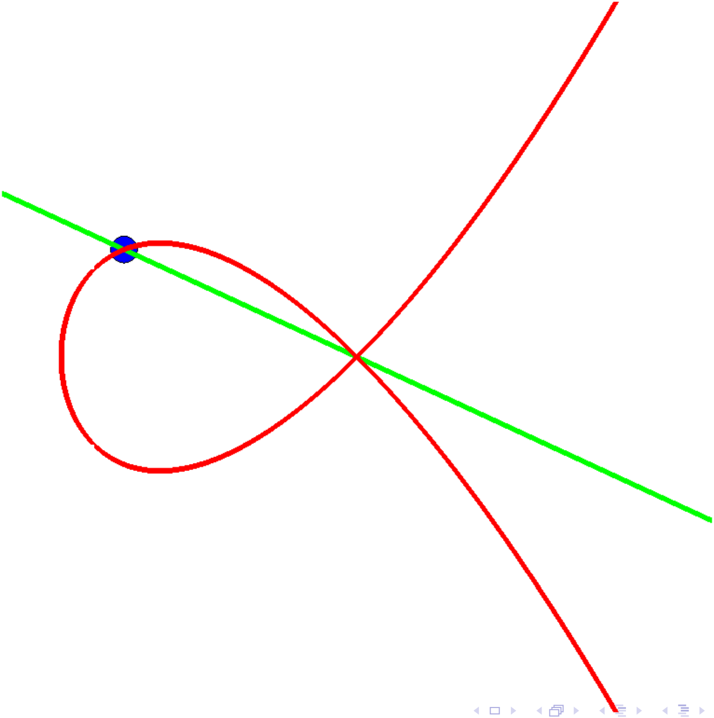


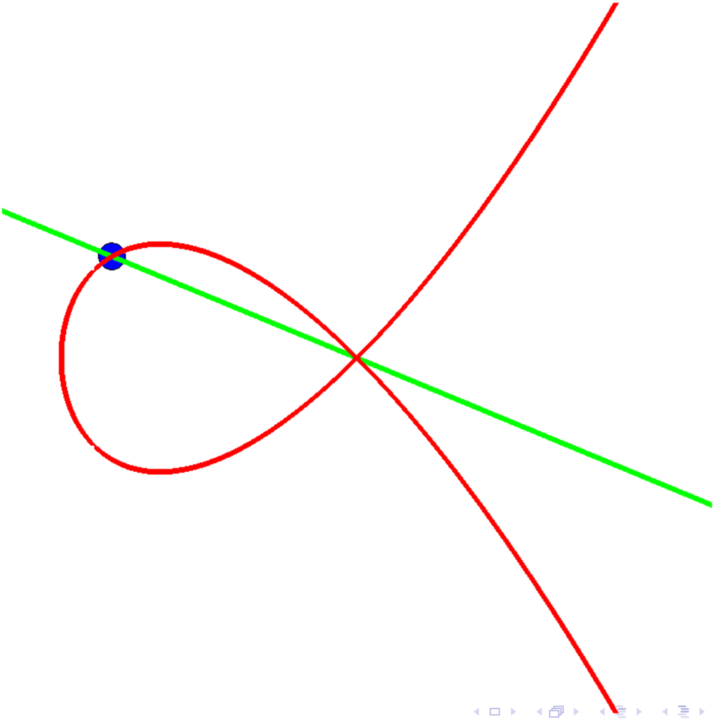


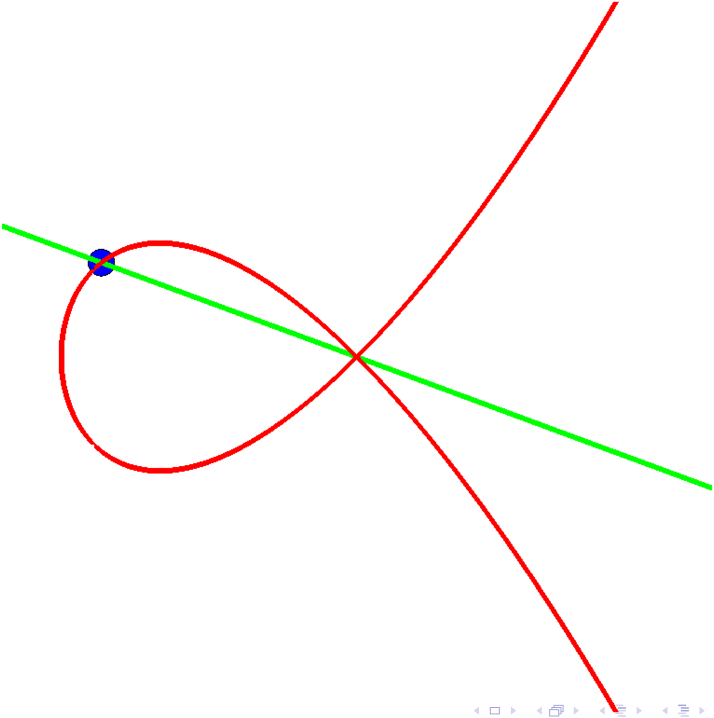


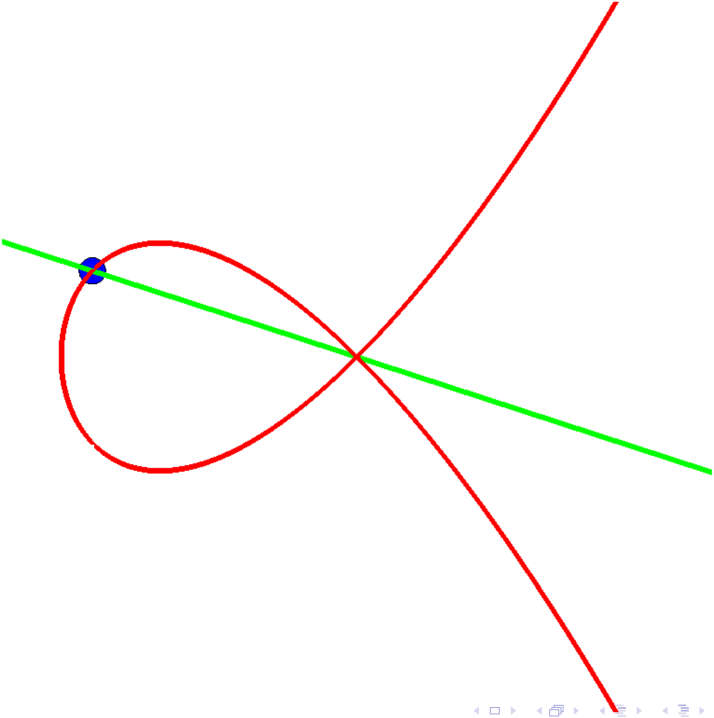


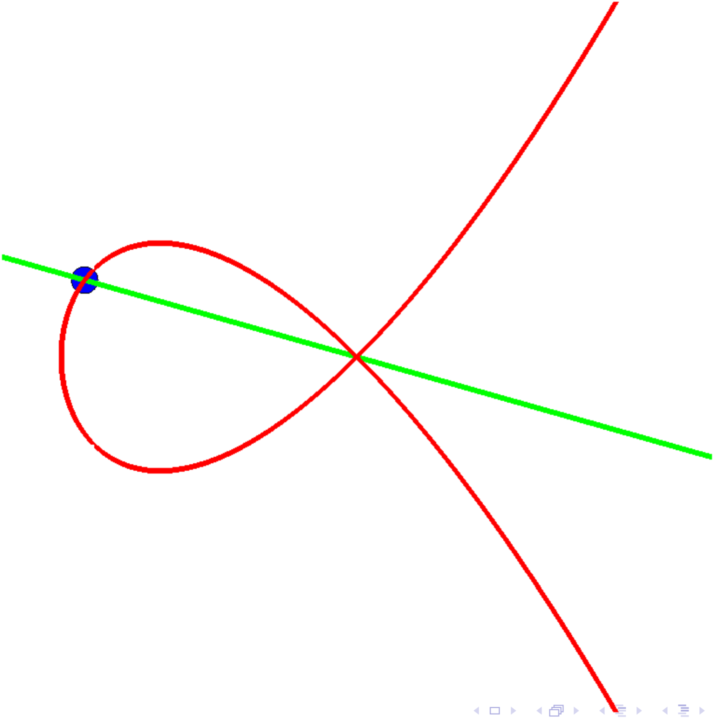


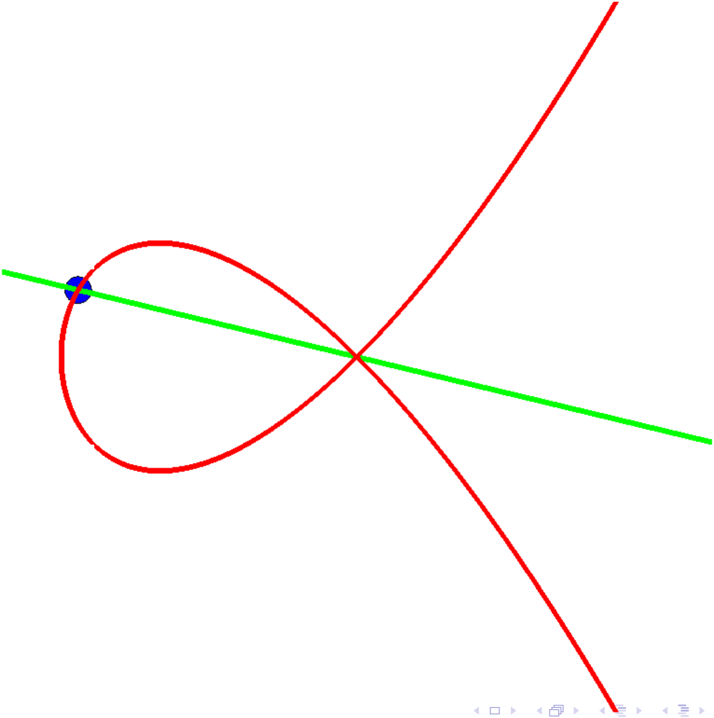


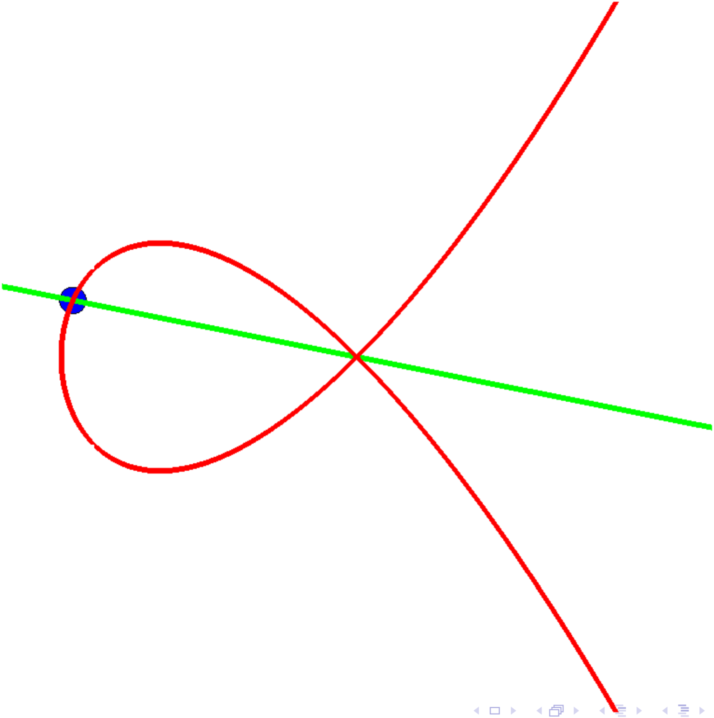


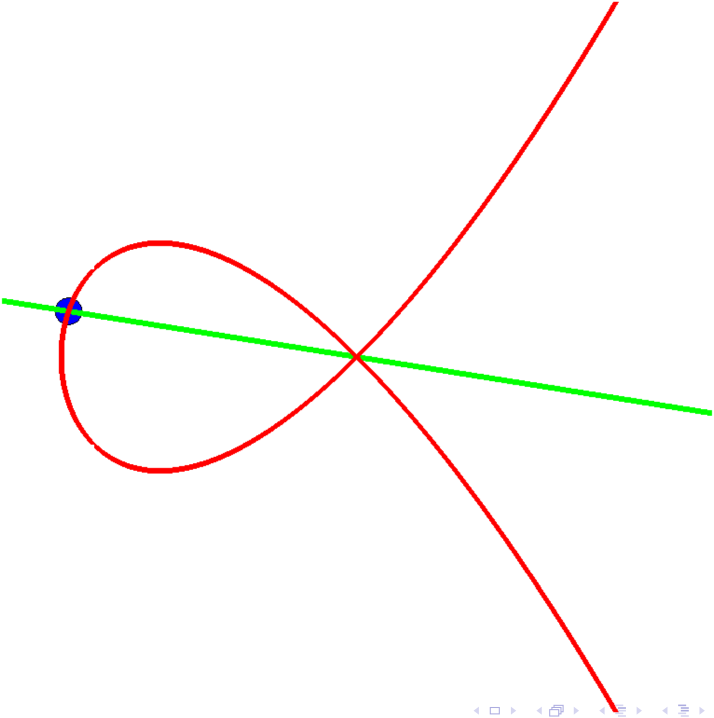


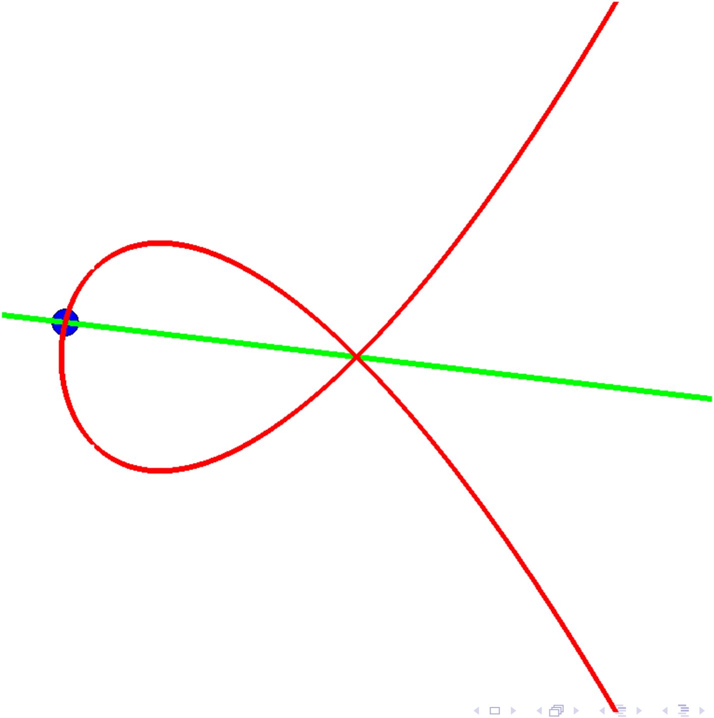


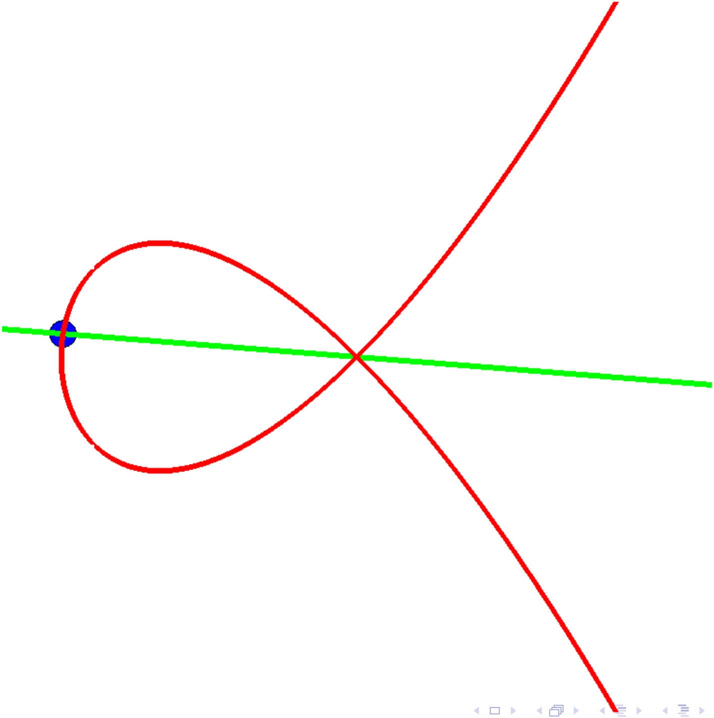


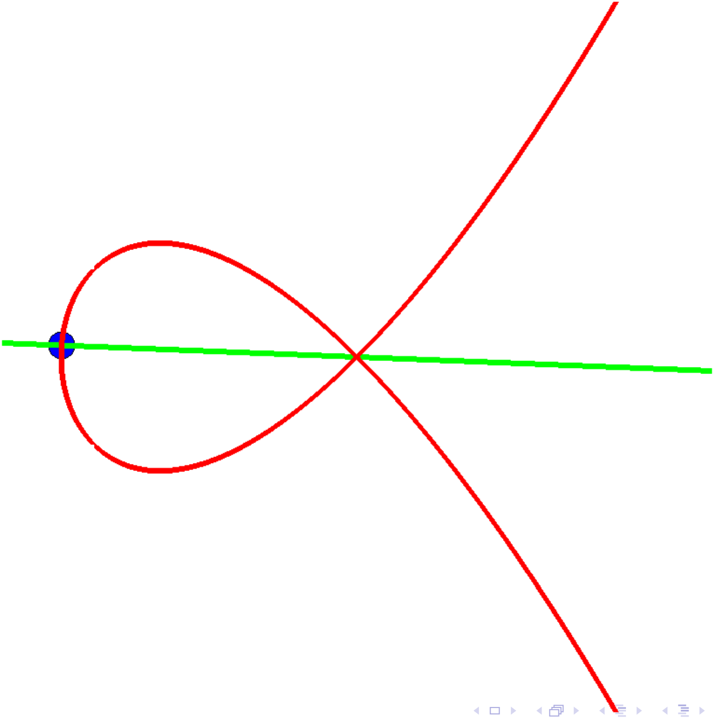


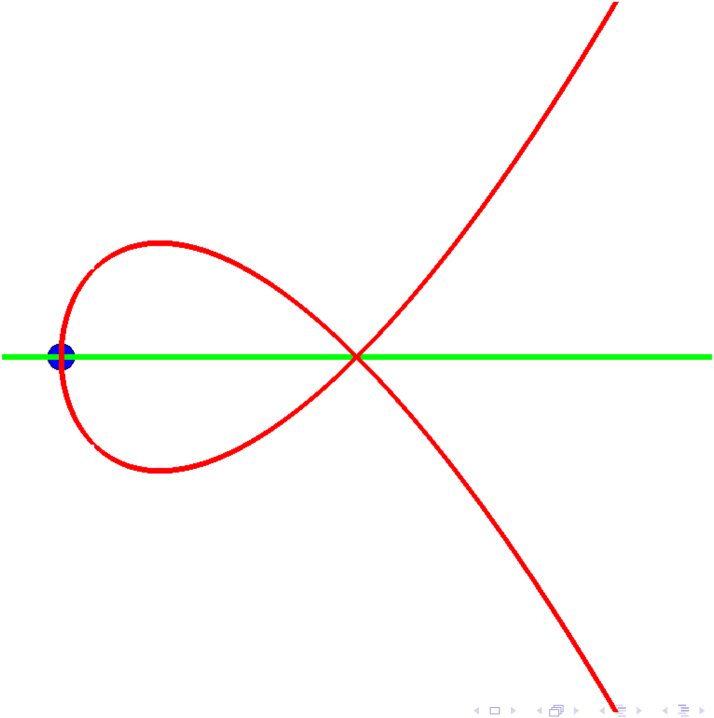


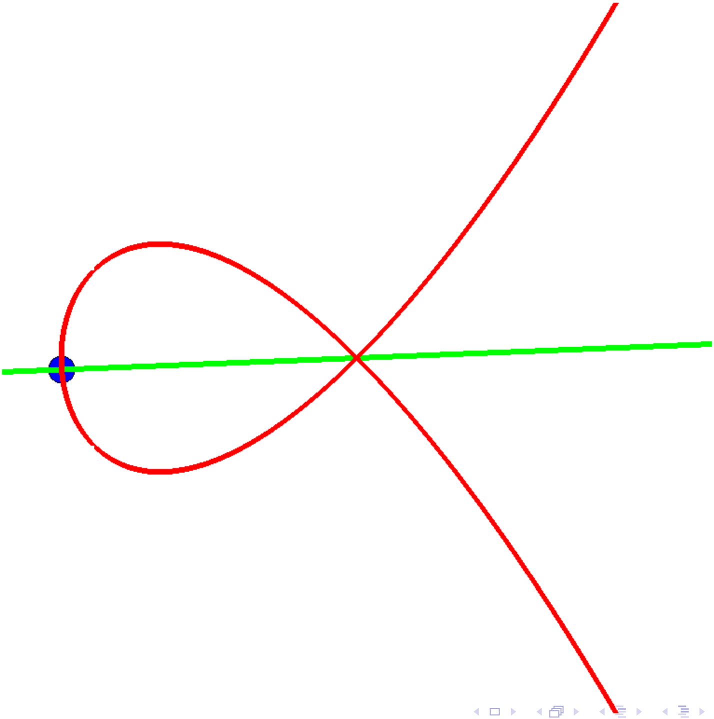


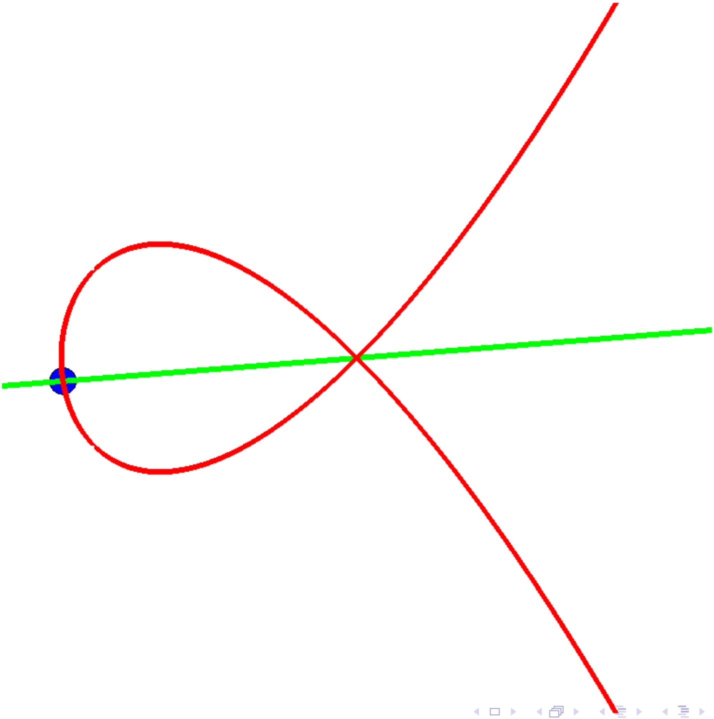


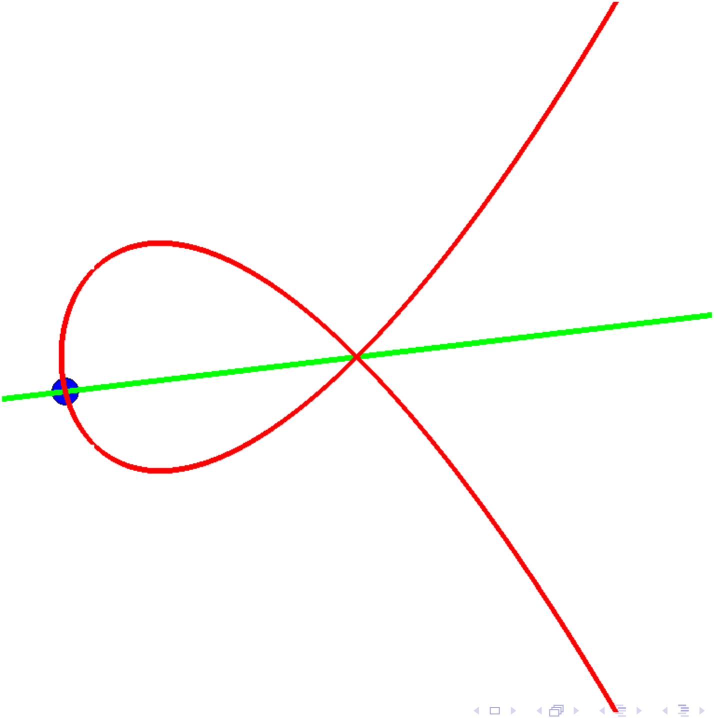


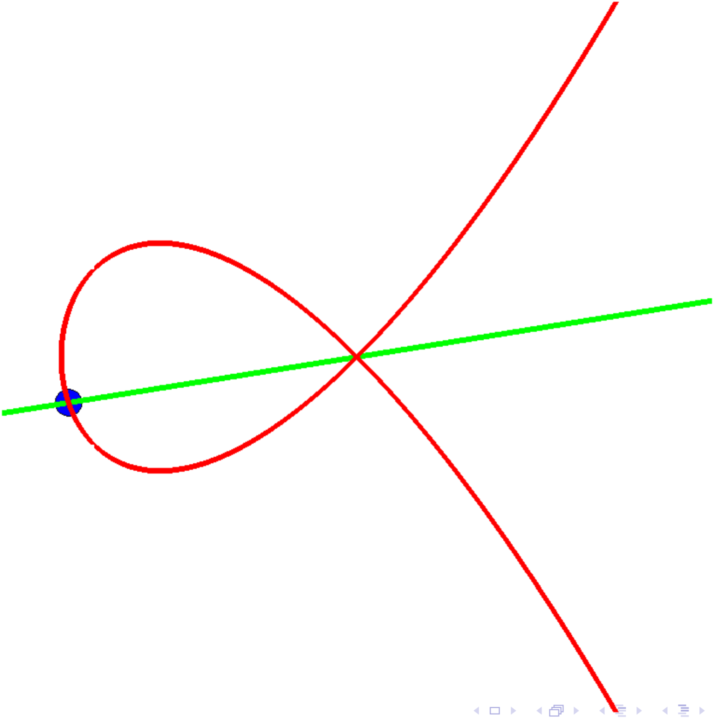


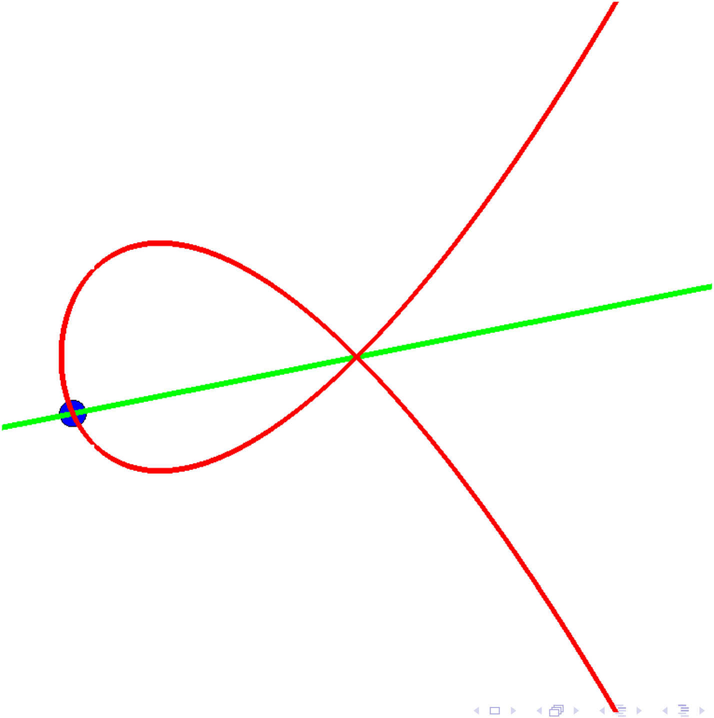


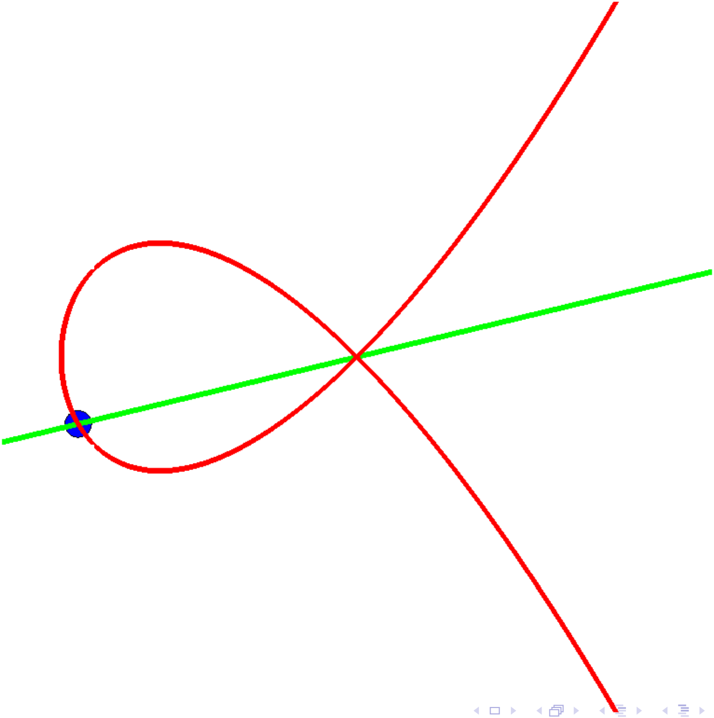


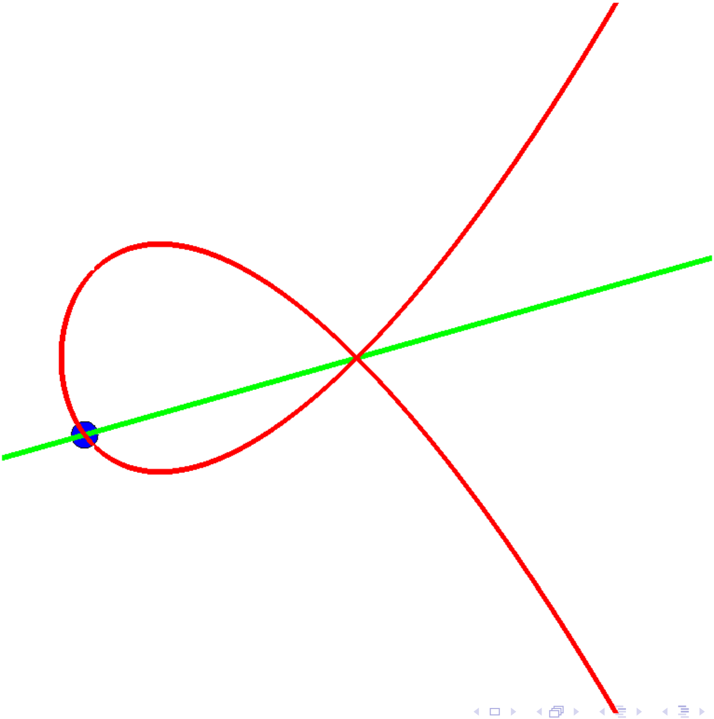


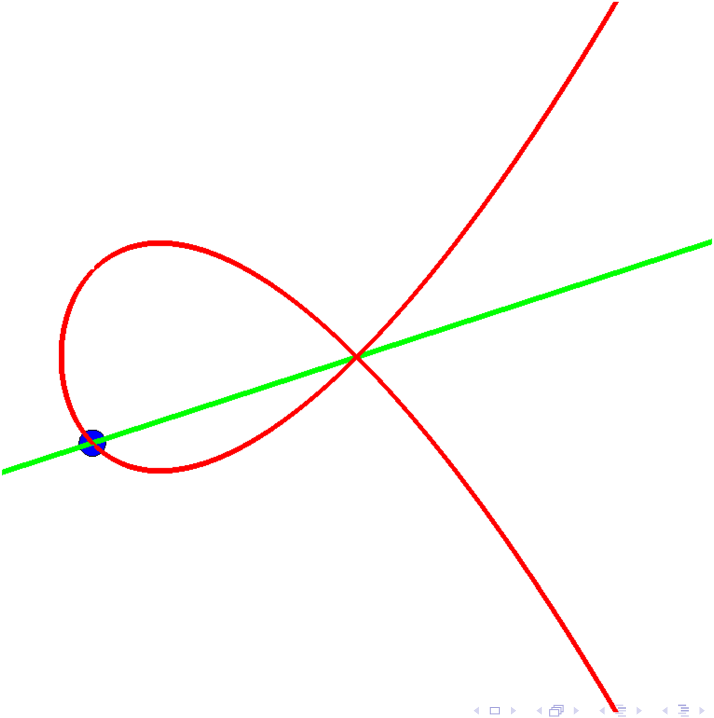


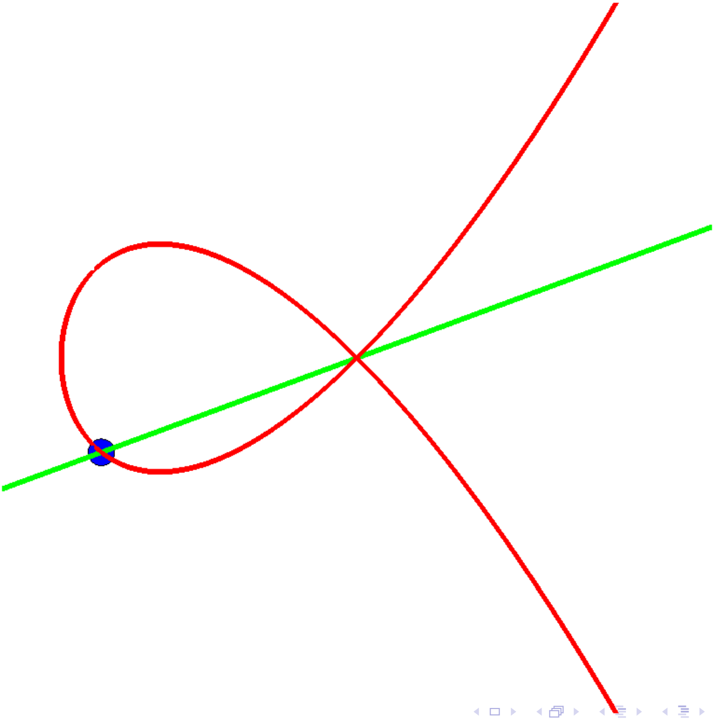


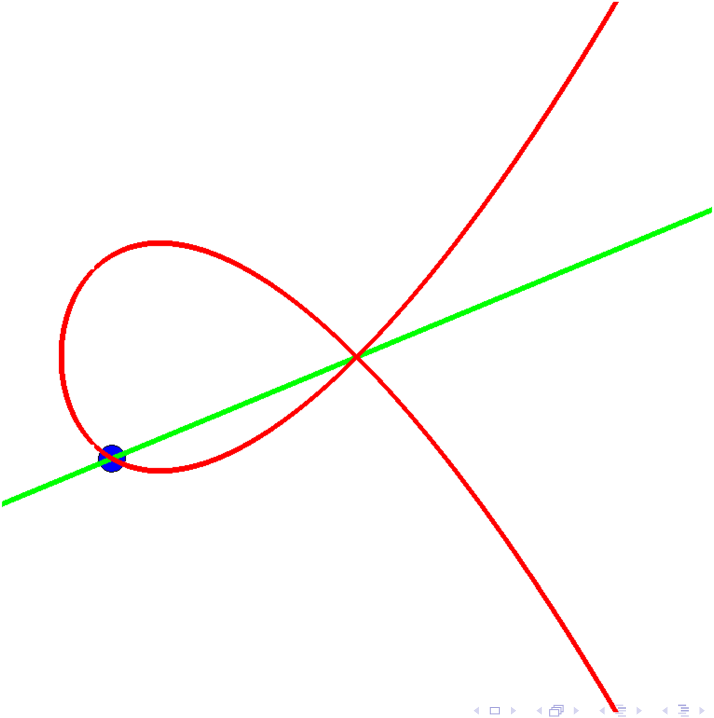


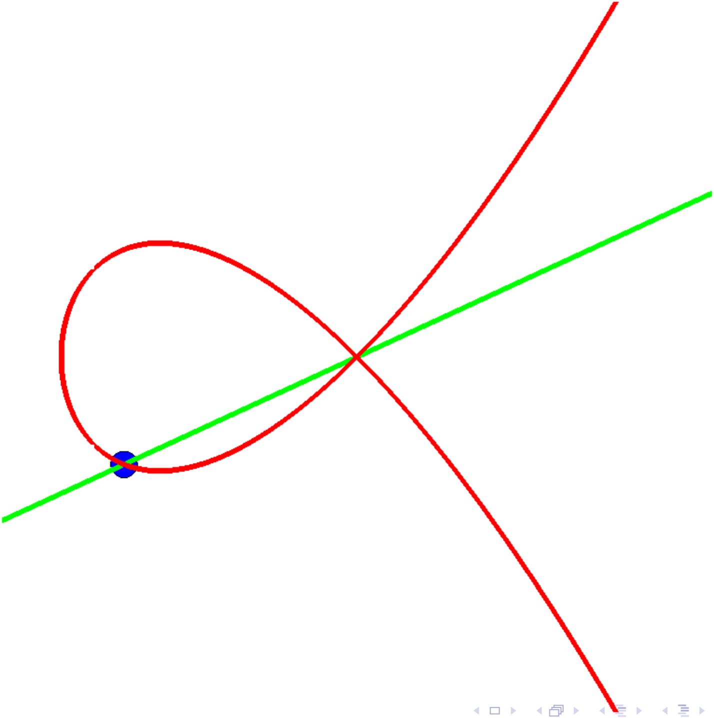


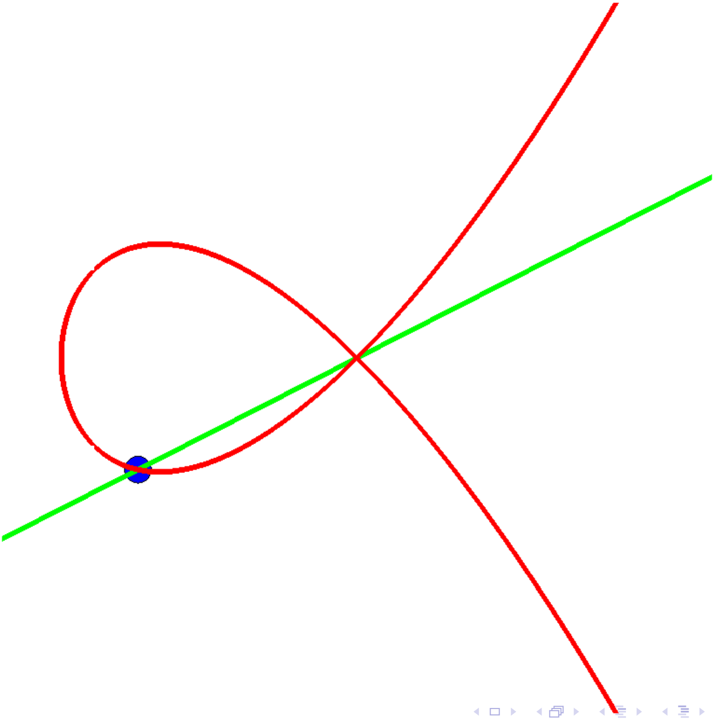


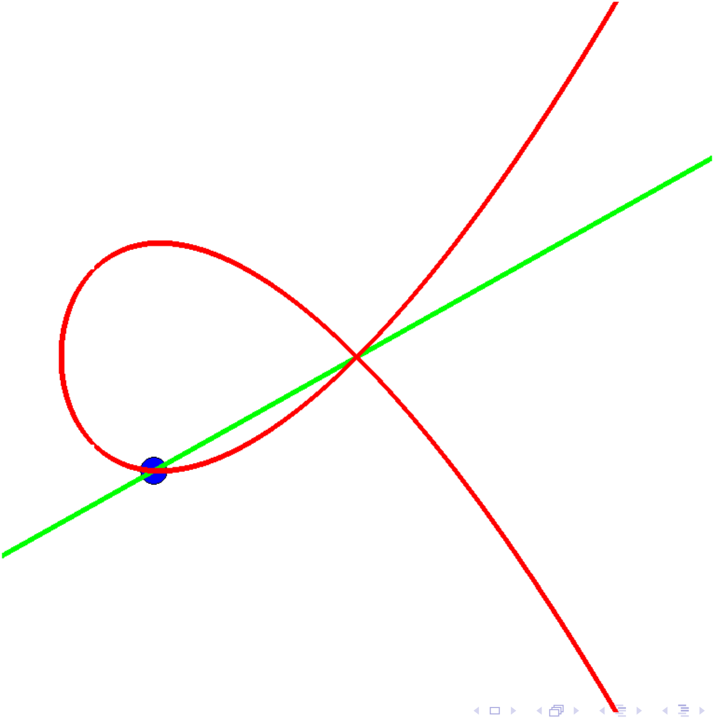


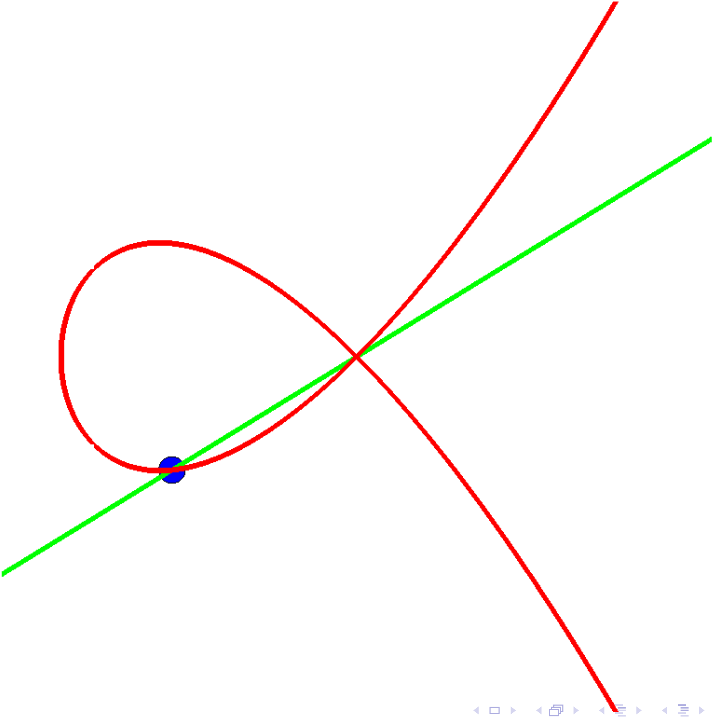


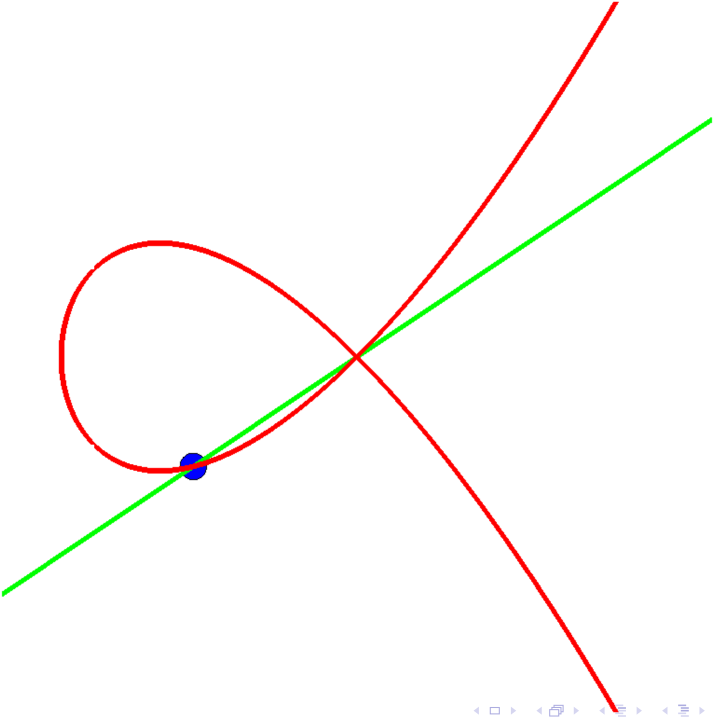


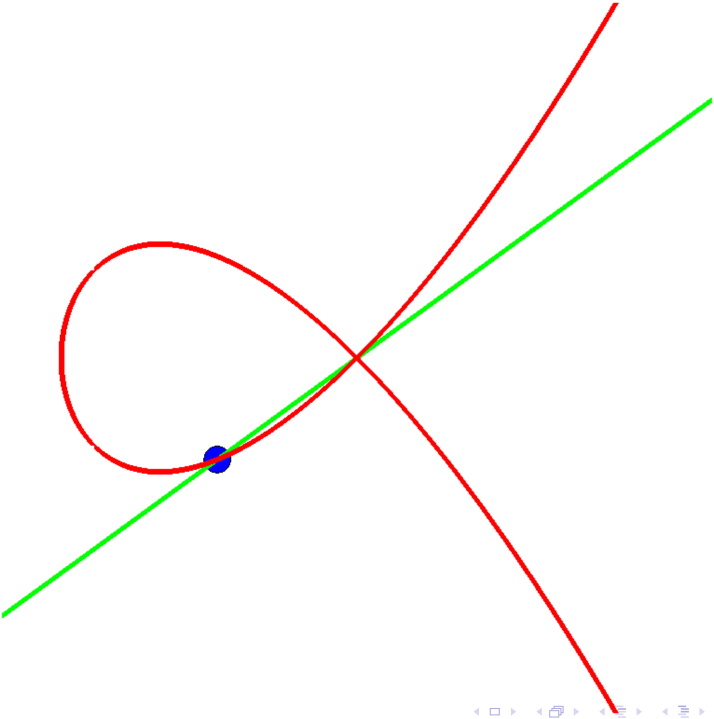


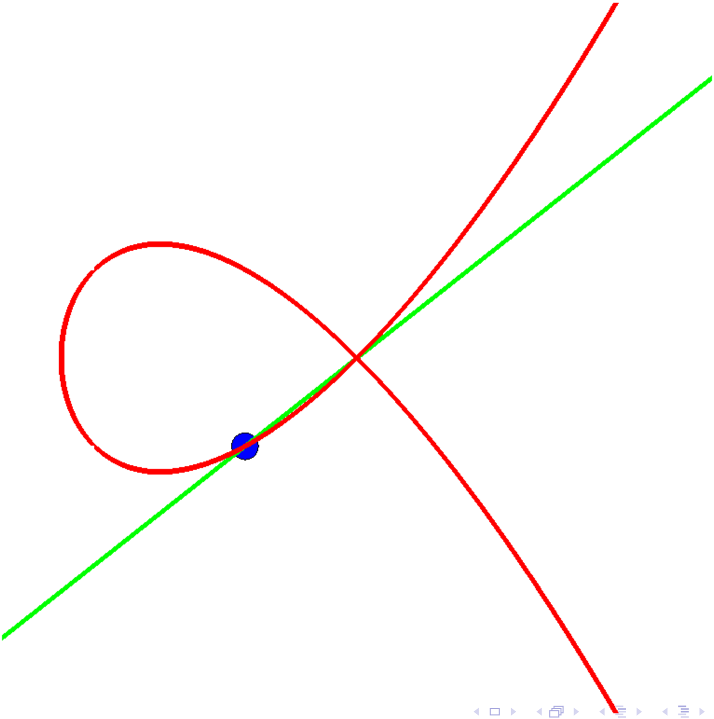


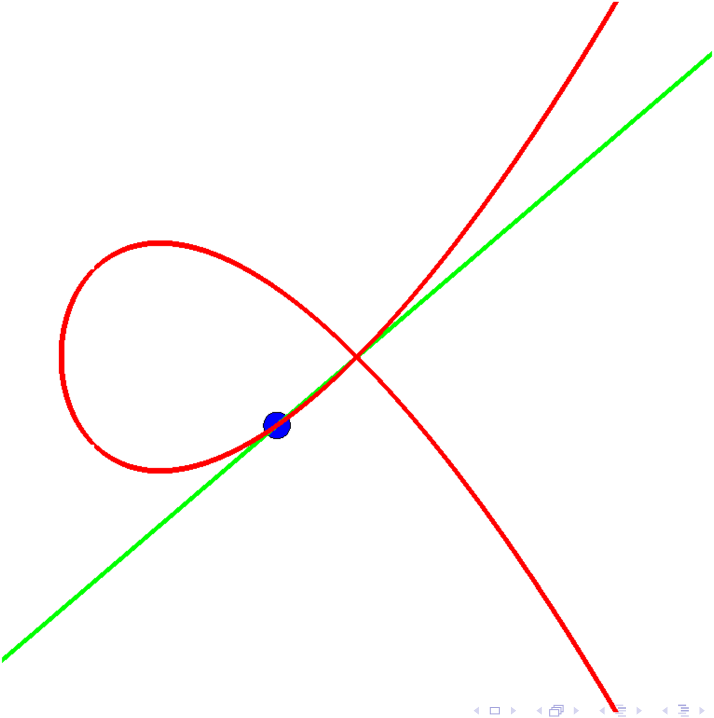


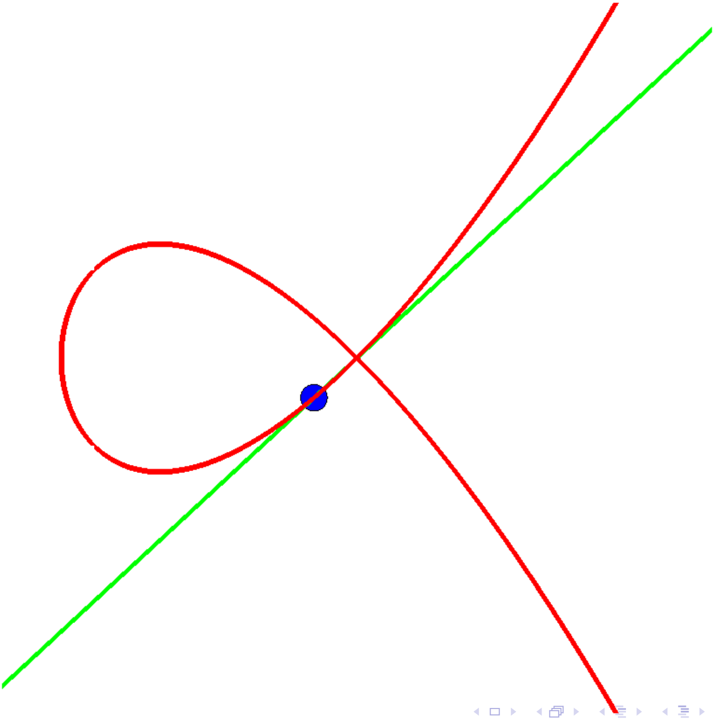


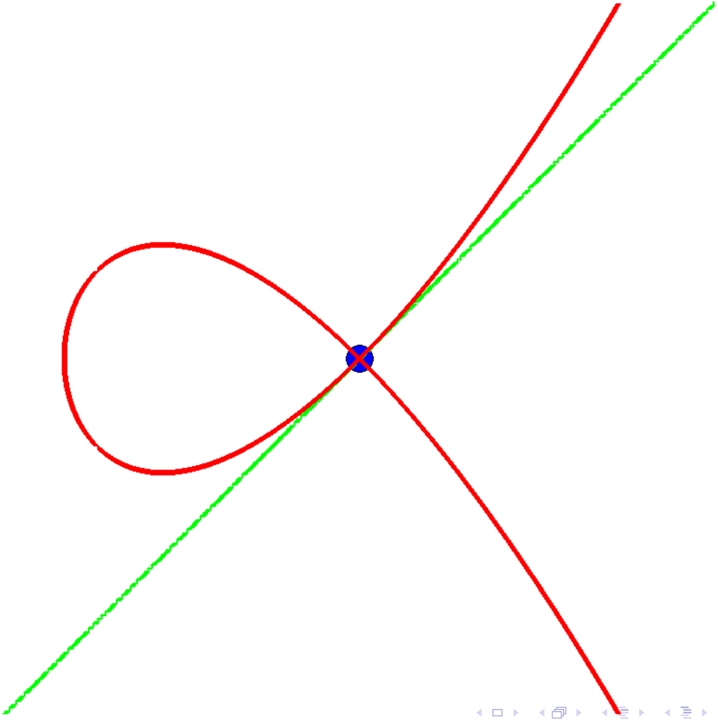


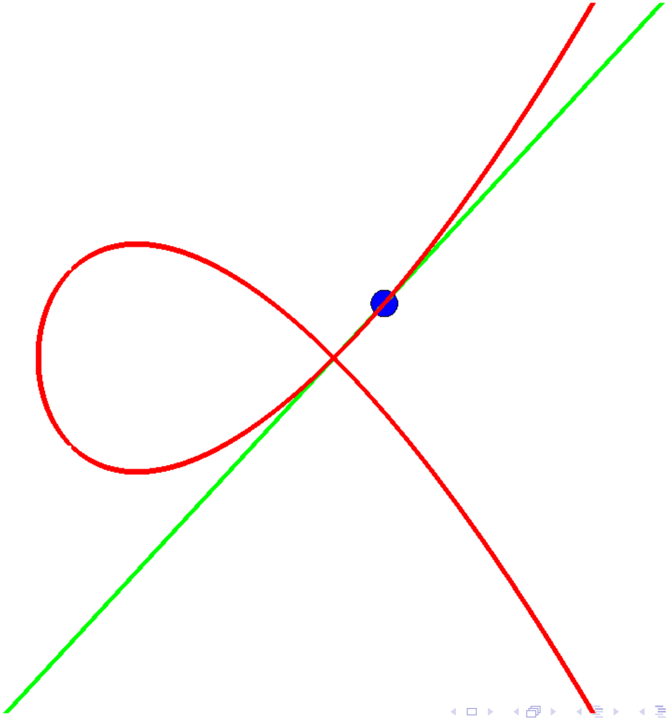


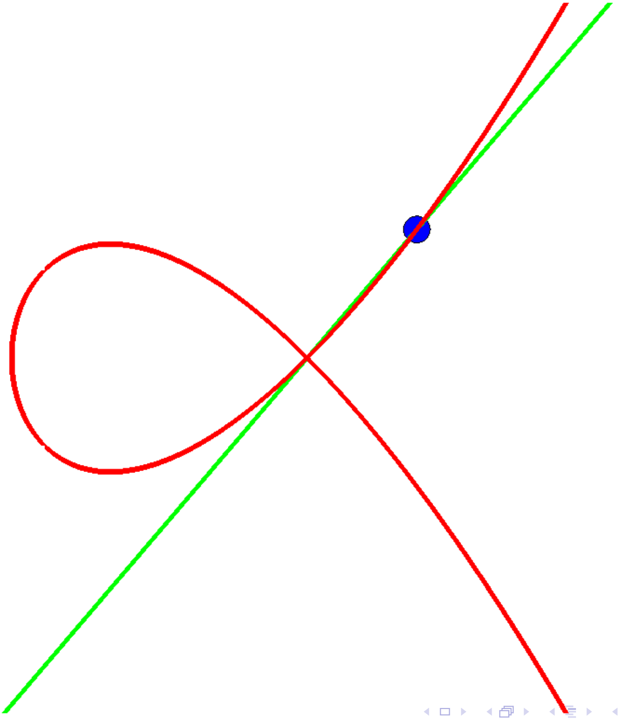


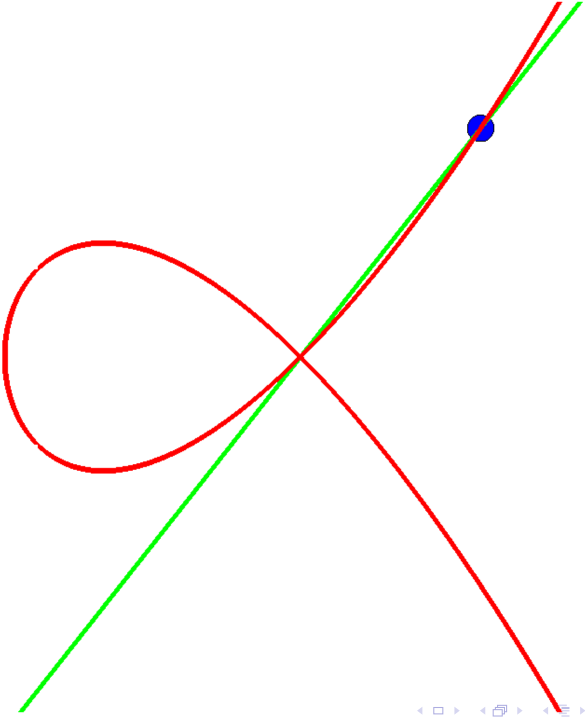


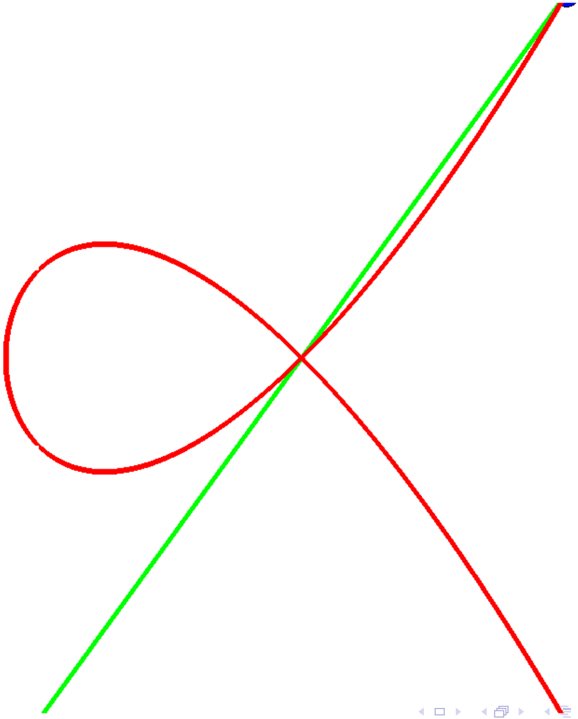


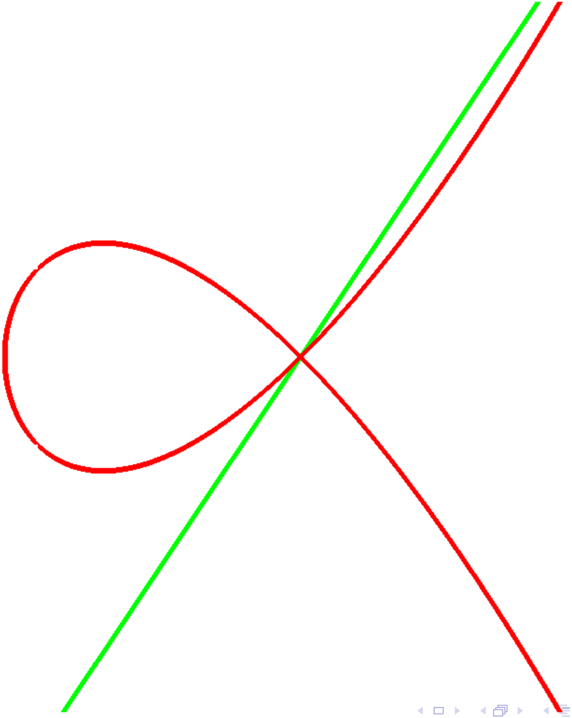


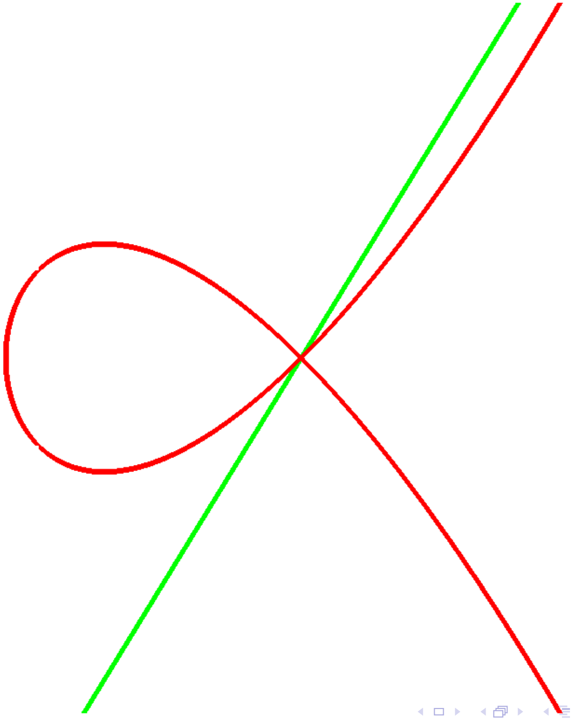


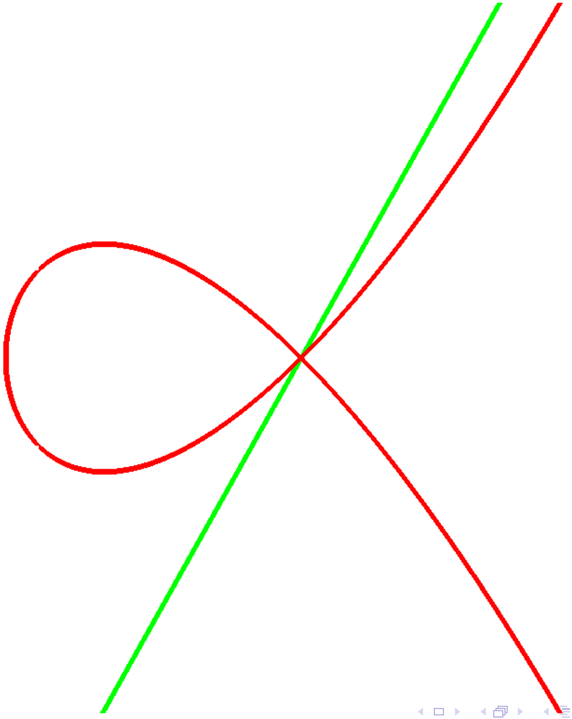


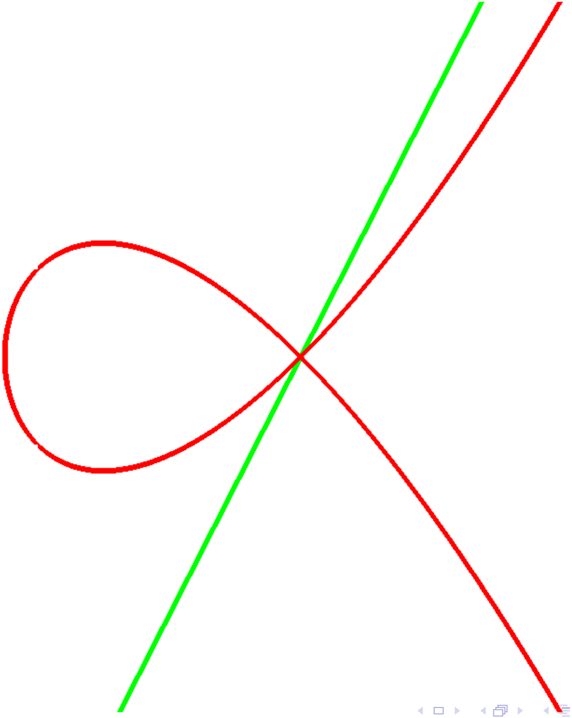


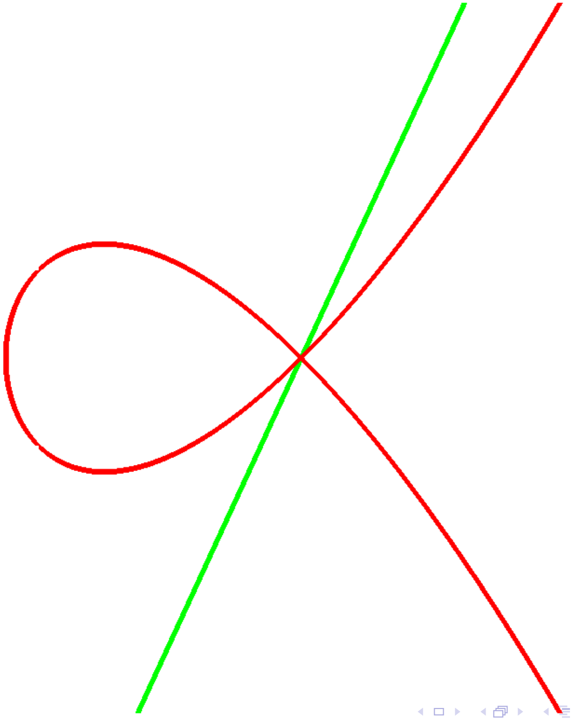


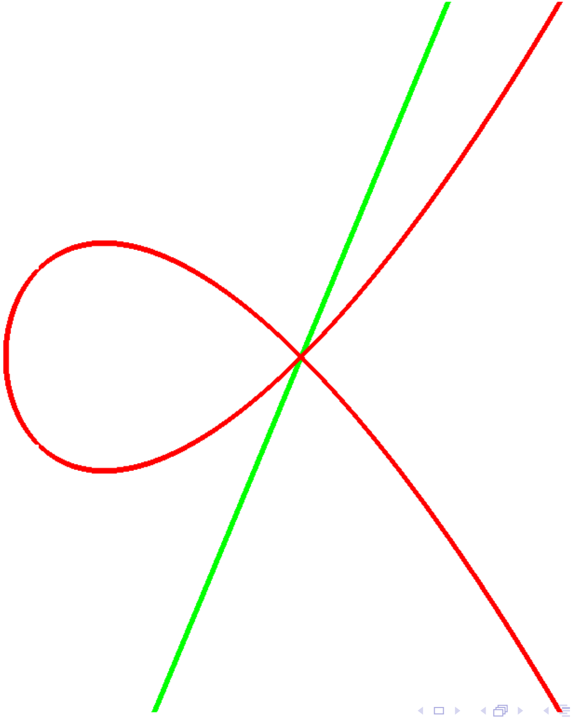


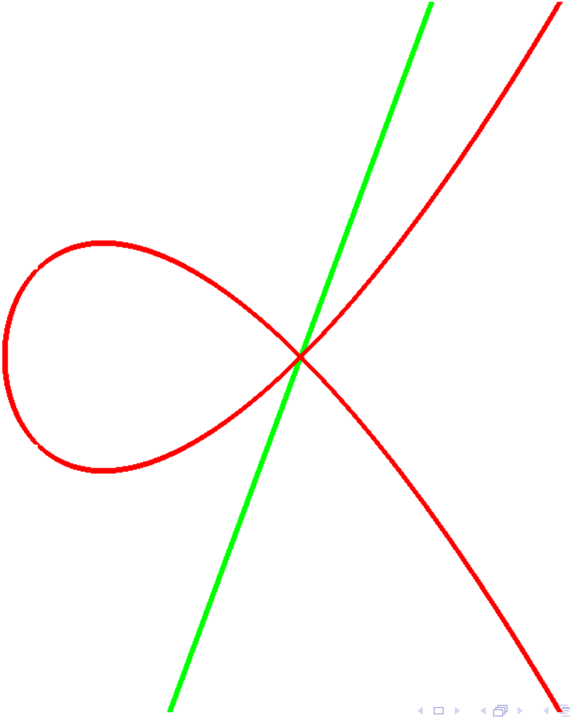


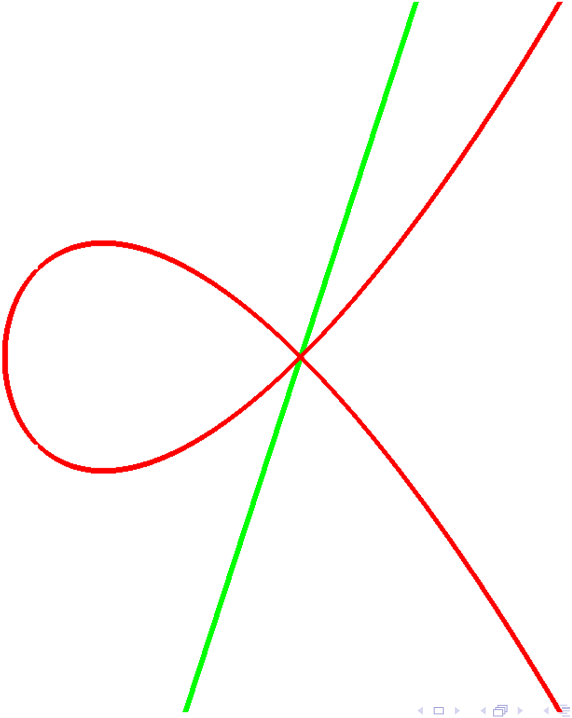


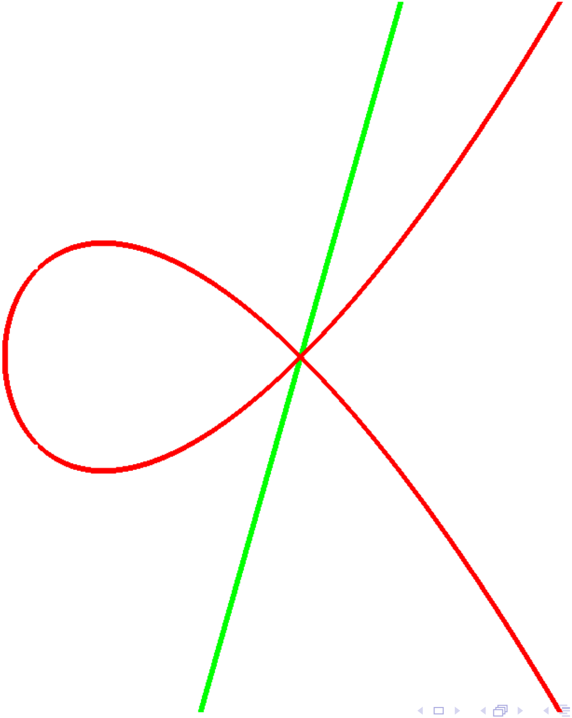


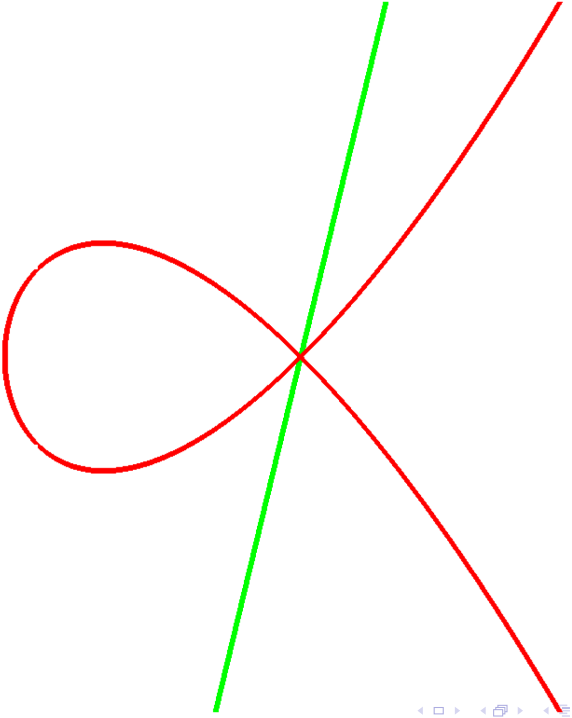


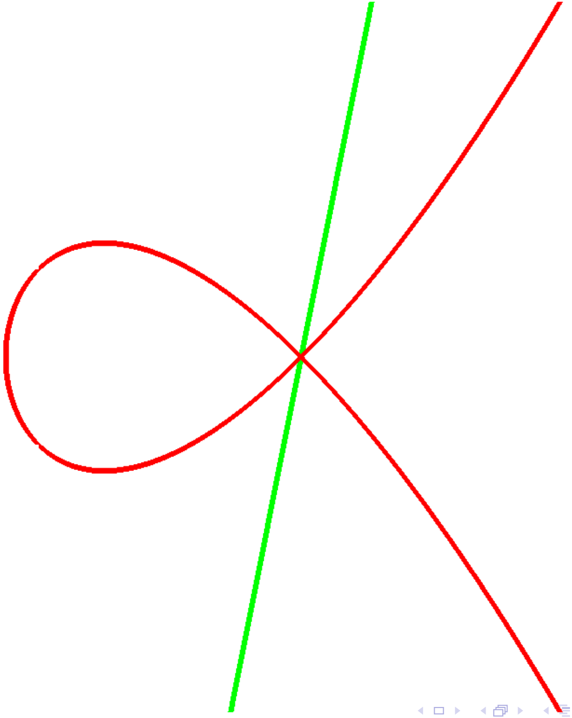


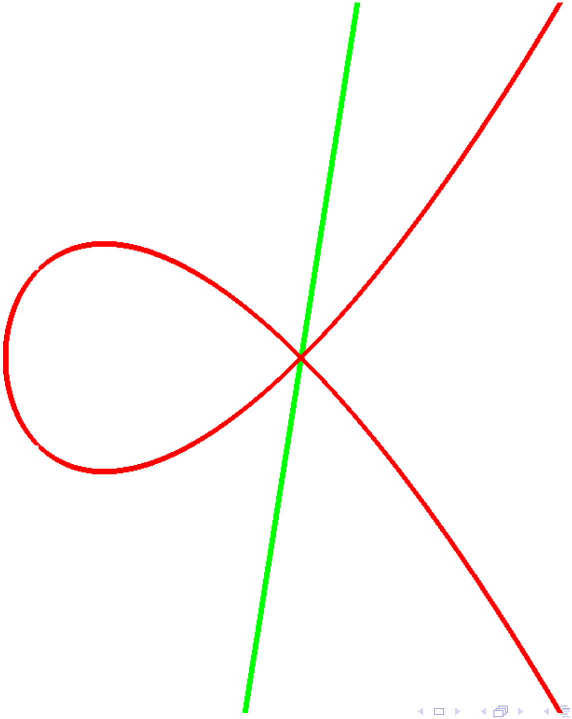


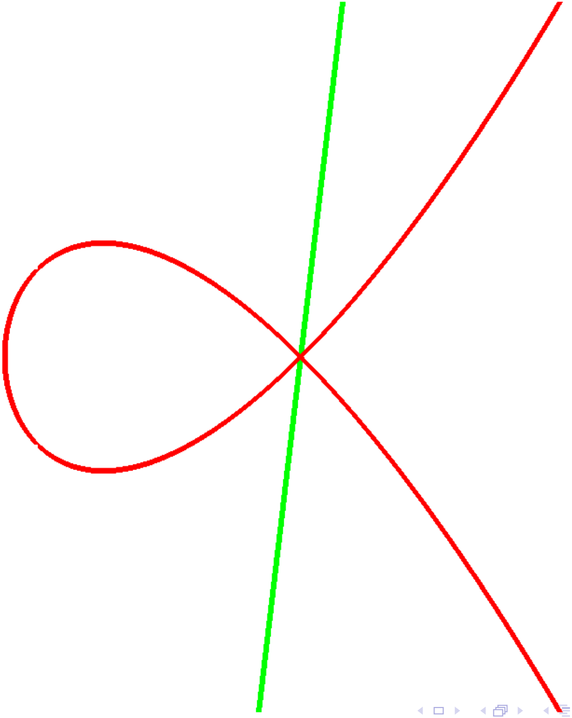


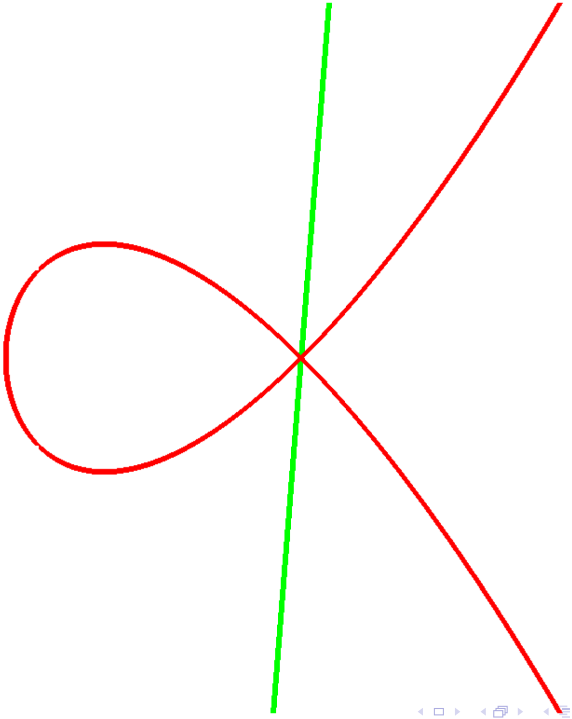


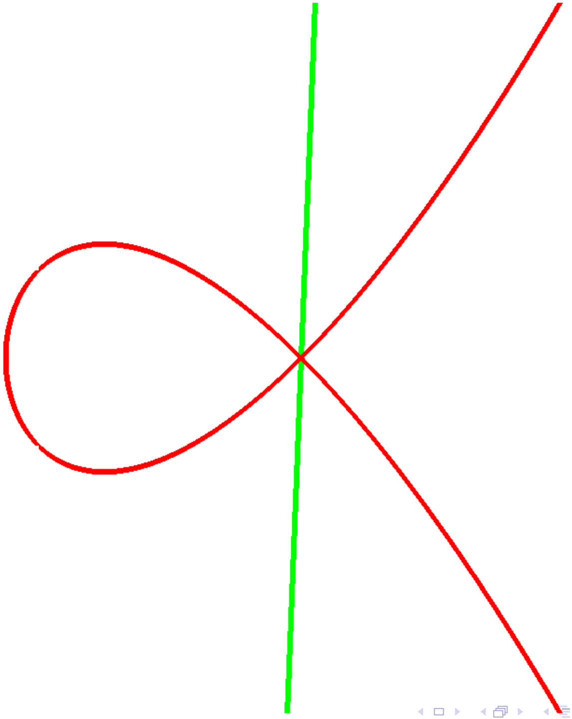


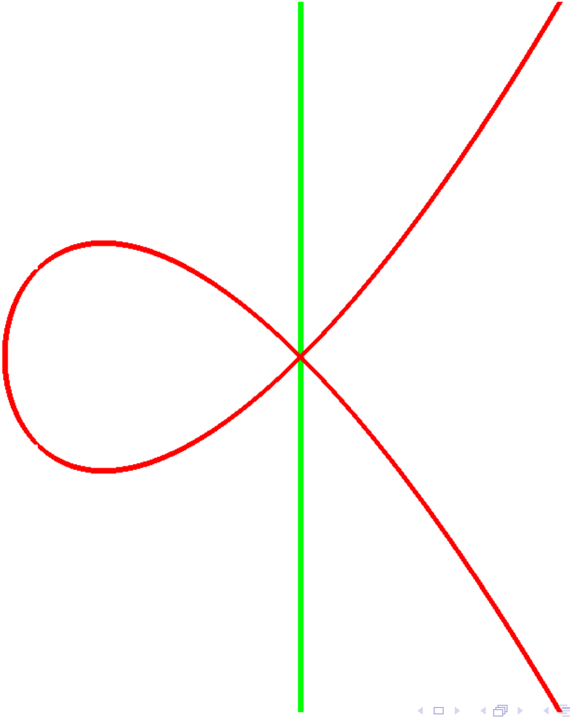












Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$.

Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$. We call A **normal** if $A = \overline{A}$.

Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$. We call A **normal** if $A = \overline{A}$.

Setup: Affine algebra $A = K[x_1, \ldots, x_n]/I$ where $I \subset K[x_1, ..., x_n]$ is ideal.

Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$. We call A **normal** if $A = \overline{A}$.

Setup: Affine algebra $A = K[x_1, \ldots, x_n]/I$ where $I \subset K[x_1, ..., x_n]$ is ideal.

Theorem (Noether)

$\overline{A}$ is a finitely generated A-module.

Example

For $C = V(I)$ where $I = \langle x^3 + x^2 - y^2 \rangle \subset K[x, y]$

$$\begin{array}{ccccc} A = K[x,y]/I & \cong & K[t^2-1, t^3-t] & \subset & K[t] \cong \overline{A} \\ \overline{x} & \mapsto & t^2-1 & & \\ \overline{y} & \mapsto & t^3-t & & \end{array}$$

Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$. We call A **normal** if $A = \overline{A}$.

Setup: Affine algebra $A = K[x_1, \ldots, x_n]/I$ where $I \subset K[x_1, ..., x_n]$ is ideal.

Theorem (Noether)

$\overline{A}$ is a finitely generated A-module.

Example

For $C = V(I)$ where $I = \langle x^3 + x^2 - y^2 \rangle \subset K[x, y]$

$$\begin{array}{rcl} A = K[x,y]/I & \cong & K[t^2-1, t^3-t] \quad \subset \quad K[t] \cong \overline{A} \\ \overline{x} & \mapsto & t^2 - 1 \\ \overline{y} & \mapsto & t^3 - t \end{array}$$

Since $K[t]$ is factorial (UFD) it is normal.

Normalization

Definition

Let A be a Noetherian domain. The **normalization** $\overline{A}$ of A is the integral closure of A in its quotient field $Q(A)$. We call A **normal** if $A = \overline{A}$.

Setup: Affine algebra $A = K[x_1, \ldots, x_n]/I$ where $I \subset K[x_1, ..., x_n]$ is ideal.

Theorem (Noether)

$\overline{A}$ is a finitely generated A-module.

Example

For $C = V(I)$ where $I = \langle x^3 + x^2 - y^2 \rangle \subset K[x, y]$

$$\begin{array}{ccccc} A = K[x,y]/I & \cong & K[t^2-1, t^3-t] & \subset & K[t] \cong \overline{A} \\ \overline{x} & \mapsto & t^2 - 1 & & \\ \overline{y} & \mapsto & t^3 - t & & \end{array}$$

Since $K[t]$ is factorial (UFD) it is normal. As an A-module $\overline{A} = \left\langle 1, \frac{\overline{y}}{\overline{x}} \right\rangle$.

Example

Theorem

Any factorial ring is normal.

Example

Theorem

Any factorial ring is normal.

Proof.

Let A be factorial and $\frac{r}{s} \in Q(A)$ integral over A.

Example

Theorem

Any factorial ring is normal.

Proof.

Let A be factorial and $\frac{r}{s} \in Q(A)$ integral over A. Then there are $a_i \in A$ with

$$\left(\frac{r}{s}\right)^n = \sum_{i=0}^{n-1} a_i \left(\frac{r}{s}\right)^i,$$

and,

Example

Theorem

Any factorial ring is normal.

Proof.

Let A be factorial and $\frac{r}{s} \in Q(A)$ integral over A. Then there are $a_i \in A$ with

$$\left(\frac{r}{s}\right)^n = \sum_{i=0}^{n-1} a_i \left(\frac{r}{s}\right)^i,$$

and, cancelling the denominator,

$$r^n = s\left(\sum_{i=0}^{n-1} a_i r^i s^{n-1-i}\right).$$

Example

Theorem

Any factorial ring is normal.

Proof.

Let A be factorial and $\frac{r}{s} \in Q(A)$ integral over A. Then there are $a_i \in A$ with

$$\left(\frac{r}{s}\right)^n = \sum_{i=0}^{n-1} a_i \left(\frac{r}{s}\right)^i,$$

and, cancelling the denominator,

$$r^n = s\left(\sum_{i=0}^{n-1} a_i r^i s^{n-1-i}\right).$$

So if p is a prime divisor of s, then also of r, which implies that $\frac{r}{s} \in A$. $\square$

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$.

Algorithm (Ideal quotients by Elimination)

$I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$.

Algorithm (Ideal quotients by Elimination)

$I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$
$I \cap \langle g \rangle = \langle g \cdot f_1, ..., g \cdot f_s \rangle \Longrightarrow I : \langle g \rangle = \langle f_1, ..., f_s \rangle$

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$.

Algorithm (Ideal quotients by Elimination)

$I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$

$I \cap \langle g \rangle = \langle g \cdot f_1, ..., g \cdot f_s \rangle \Longrightarrow I : \langle g \rangle = \langle f_1, ..., f_s \rangle$

$I, J \subset R \Longrightarrow I \cap J = (t \cdot I + (1 - t) \cdot J) \cap R$

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$.

Algorithm (Ideal quotients by Elimination)

$I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$
$I \cap \langle g \rangle = \langle g \cdot f_1, ..., g \cdot f_s \rangle \Longrightarrow I : \langle g \rangle = \langle f_1, ..., f_s \rangle$
$I, J \subset R \Longrightarrow I \cap J = (t \cdot I + (1-t) \cdot J) \cap R$

Lemma

If $J \subset A$ is an ideal and $0 \neq g \in J$, then

Key Lemma

Definition

For ideals $I_j \subset A$ the **ideal quotient** is $(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$.

Algorithm (Ideal quotients by Elimination)

$I : \langle g_1, g_2 \rangle = (I : g_1) \cap (I : g_2)$
$I \cap \langle g \rangle = \langle g \cdot f_1, ..., g \cdot f_s \rangle \Longrightarrow I : \langle g \rangle = \langle f_1, ..., f_s \rangle$
$I, J \subset R \Longrightarrow I \cap J = (t \cdot I + (1 - t) \cdot J) \cap R$

Lemma

If $J \subset A$ is an ideal and $0 \neq g \in J$, then

$$\begin{array}{ccccccc} A & \hookrightarrow & \mathrm{Hom}_A(J, J) & \cong & \frac{1}{g}(gJ :_A J) & \subset & \overline{A} \\ a & \mapsto & a\cdot & & & & \\ & & \varphi & \mapsto & \frac{\varphi(g)}{g} & & \end{array}$$

Key Lemma

Proof.

Let $J = \langle g_1, \ldots, g_s \rangle$ and $b \in (gJ :_A J)$.

Key Lemma

Proof.

Let $J = \langle g_1, \ldots, g_s \rangle$ and $b \in (gJ :_A J)$. By

$$bJ \subset gJ$$

there are $b_{ij} \in \langle g \rangle$ with

$$bg_j = \sum_i b_{ij} g_i.$$

Key Lemma

Proof.

Let $J = \langle g_1, \ldots, g_s \rangle$ and $b \in (gJ :_A J)$. By

$$bJ \subset gJ$$

there are $b_{ij} \in \langle g \rangle$ with

$$bg_j = \sum\nolimits_i b_{ij} g_i.$$

By Cayley-Hamilton, $b\cdot$ is a zero of $\chi(t) = \det(t \cdot E - (b_{ij}))$,

Key Lemma

Proof.

Let $J = \langle g_1, \ldots, g_s \rangle$ and $b \in (gJ :_A J)$. By

$$bJ \subset gJ$$

there are $b_{ij} \in \langle g \rangle$ with

$$bg_j = \sum_i b_{ij} g_i.$$

By Cayley-Hamilton, $b\cdot$ is a zero of $\chi(t) = \det(t \cdot E - (b_{ij}))$, so there are

$$a_i \in \langle g \rangle^i \quad \text{with} \quad \sum_{i=0}^{s} a_i b^{s-i} = 0 \quad \text{and} \quad a_0 = 1$$

Key Lemma

Proof.

Let $J = \langle g_1, \ldots, g_s \rangle$ and $b \in (gJ :_A J)$. By

$$bJ \subset gJ$$

there are $b_{ij} \in \langle g \rangle$ with

$$bg_j = \sum_i b_{ij} g_i.$$

By Cayley-Hamilton, $b\cdot$ is a zero of $\chi(t) = \det(t \cdot E - (b_{ij}))$, so there are

$$a_i \in \langle g \rangle^i \quad \text{with} \quad \sum_{i=0}^{s} a_i b^{s-i} = 0 \quad \text{and} \quad a_0 = 1$$

hence

$$\sum_{i=0}^{s} \frac{a_i}{g^i} \left(\frac{b}{g} \right)^{s-i} = 0 \quad \text{with} \quad \frac{a_i}{g^i} \in A.$$

□

Non-normal and singular locus

For simplicity, assume $V(I)$ is curve. Then the **non-normal locus** $N(A)$ is equal to the **singular locus** $\operatorname{Sing}(A)$.

Non-normal and singular locus

For simplicity, assume $V(I)$ is curve. Then the **non-normal locus** $N(A)$ is equal to the **singular locus** $\mathrm{Sing}(A)$. In general, $N(A) \subset \mathrm{Sing}(A)$.

Non-normal and singular locus

For simplicity, assume $V(I)$ is curve. Then the **non-normal locus** $N(A)$ is equal to the **singular locus** $\mathrm{Sing}(A)$. In general, $N(A) \subset \mathrm{Sing}(A)$.

Definition

For an ideal $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$, the **Jacobian ideal** $\mathrm{Jac}(I)$ is generated by the $c \times c$ minors of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial x_1} & \cdots & \frac{\partial f_s}{\partial x_n} \end{pmatrix}$$

where $c = n - \dim(X)$ is the **codimension** of $X = V(I)$.

Non-normal and singular locus

For simplicity, assume $V(I)$ is curve. Then the **non-normal locus** $N(A)$ is equal to the **singular locus** $\text{Sing}(A)$. In general, $N(A) \subset \text{Sing}(A)$.

Definition

For an ideal $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$, the **Jacobian ideal** $\text{Jac}(I)$ is generated by the $c \times c$ minors of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial x_1} & \cdots & \frac{\partial f_s}{\partial x_n} \end{pmatrix}$$

where $c = n - \dim(X)$ is the **codimension** of $X = V(I)$. Then

$$\text{Sing}(A) = V(\text{Jac}(I) + I).$$

Example

For $I = \langle x^4 + x^5 - y^2 \rangle$ we have $\text{Jac}(I) + I = \langle x^3, y \rangle$.

Grauert-Remmert Criterion

Definition

The **radical** of an ideal $I \subset A$ is

$$\sqrt{I} = \{f \in A \mid \exists a \in \mathbb{N} \text{ with } f^a \in I\}$$

Example

$\sqrt{\langle x^3, y \rangle} = \langle x, y \rangle$.

Grauert-Remmert Criterion

Definition

The **radical** of an ideal $I \subset A$ is

$$\sqrt{I} = \{f \in A \mid \exists a \in \mathbb{N} \text{ with } f^a \in I\}$$

Example

$\sqrt{\langle x^3, y\rangle} = \langle x, y\rangle$.

Theorem (Grauert-Remmert)

Let $0 \neq J \subset A = K[x_1, ..., x_n]/I$ *be an ideal with* $J = \sqrt{J}$

Grauert-Remmert Criterion

Definition

The **radical** of an ideal $I \subset A$ is

$$\sqrt{I} = \{f \in A \mid \exists a \in \mathbb{N} \text{ with } f^a \in I\}$$

Example

$\sqrt{\langle x^3, y\rangle} = \langle x, y\rangle$.

Theorem (Grauert-Remmert)

Let $0 \neq J \subset A = K[x_1, \ldots, x_n]/I$ *be an ideal with* $J = \sqrt{J}$ *and*

$$N(A) \subset V(J).$$

Grauert-Remmert Criterion

Definition

The **radical** of an ideal $I \subset A$ is

$$\sqrt{I} = \{f \in A \mid \exists a \in \mathbb{N} \text{ with } f^a \in I\}$$

Example

$\sqrt{\langle x^3, y \rangle} = \langle x, y \rangle$.

Theorem (Grauert-Remmert)

Let $0 \neq J \subset A = K[x_1, ..., x_n]/I$ *be an ideal with* $J = \sqrt{J}$ *and*

$$N(A) \subset V(J).$$

Then A *is normal iff the inclusion*

$$\begin{array}{ccc} A & \hookrightarrow & \mathrm{Hom}_A(J, J) \\ a & \mapsto & (b \mapsto ab) \end{array}$$

is an isomorphism.

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneqq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneqq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

This gives algorithm [de Jong, 98], [Greuel, Laplagne, Seelisch, 2010]:

Algorithm

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

This gives algorithm [de Jong, 98], [Greuel, Laplagne, Seelisch, 2010]:

Algorithm

Starting from $A_0 = A$ and $J_0 = J$,

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

This gives algorithm [de Jong, 98], [Greuel, Laplagne, Seelisch, 2010]:

Algorithm

Starting from $A_0 = A$ and $J_0 = J$, setting

$$A_{i+1} = \tfrac{1}{g}(gJ_i :_{A_i} J_i) \qquad J_i = \sqrt{JA_i}$$

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

This gives algorithm [de Jong, 98], [Greuel, Laplagne, Seelisch, 2010]:

Algorithm

Starting from $A_0 = A$ and $J_0 = J$, setting

$$A_{i+1} = \tfrac{1}{g}(gJ_i :_{A_i} J_i) \qquad J_i = \sqrt{JA_i}$$

we get a chain of extensions of reduced Noetherian rings

$$A = A_0 \subset \cdots \subset A_i \subset \cdots \subset A_m = A_{m+1} = \overline{A}.$$

Terminates since A is Noetherian. By Grauert-Remmert $A_m = \overline{A}$,

Normalization Algorithm

If A is not normal, then for $J = \sqrt{\mathrm{Jac}(I) + I}$ by Grauert-Remmert

$$A \subsetneq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset Q(A).$$

This gives algorithm [de Jong, 98], [Greuel, Laplagne, Seelisch, 2010]:

Algorithm

Starting from $A_0 = A$ and $J_0 = J$, setting

$$A_{i+1} = \tfrac{1}{g}(gJ_i :_{A_i} J_i) \qquad J_i = \sqrt{JA_i}$$

we get a chain of extensions of reduced Noetherian rings

$$A = A_0 \subset \cdots \subset A_i \subset \cdots \subset A_m = A_{m+1} = \overline{A}.$$

Terminates since A is Noetherian. By Grauert-Remmert $A_m = \overline{A}$, using:

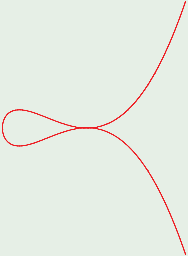
Lemma

$N(A_i) \subset V(J_i)$

Normalization Algorithm

Example

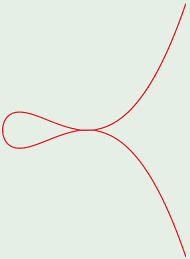
For $I = \langle x^4 + x^5 - y^2 \rangle$



Normalization Algorithm

Example

For $I = \left\langle x^4 + x^5 - y^2 \right\rangle$



the first step yields

$$A_1 = \frac{1}{x}\,(xJ : x) = \frac{1}{x}\,\langle x, y\rangle =_A \left\langle 1, \frac{y}{x} \right\rangle$$

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

```
                     SINGULAR                              /   Development
 A Computer Algebra System for Polynomial Computations    /    version 4
                                                        0<
 by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann   \   Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern     \
```

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

```
                     SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations       /    version 4
                                                           0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann    \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern       \
> ring R = 0,(x,y),lp;
```

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

```
                     SINGULAR                              /   Development
 A Computer Algebra System for Polynomial Computations    /    version 4
                                                        0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann  \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern     \
> ring R = 0,(x,y),lp;
> ideal I = x^4 - y^2 + x^5;
```

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

```
                     SINGULAR                                 /   Development
 A Computer Algebra System for Polynomial Computations       /    version 4
                                                           0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann    \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern       \
> ring R = 0,(x,y),lp;
> ideal I = x^4 - y^2 + x^5;
> LIB "normal.lib";
```

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

```
                         SINGULAR                              /   Development
 A Computer Algebra System for Polynomial Computations        /    version 4
                                                            0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann     \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern        \
> ring R = 0,(x,y),lp;
> ideal I = x^4 - y^2 + x^5;
> LIB "normal.lib";
> list nor = normal(I,"var1");
```

Normalization Algorithm

To obtain $\overline{A}$, one more iteration is needed, leading to $A_2 =_A \left\langle 1, \frac{y}{x^2} \right\rangle$:

Example

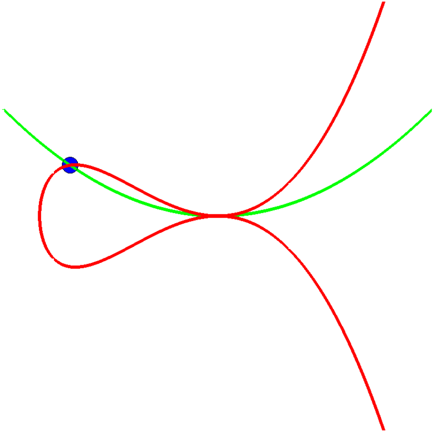
```
                           SINGULAR                              /   Development
 A Computer Algebra System for Polynomial Computations          /    version 4
                                                              0<
 by:  W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann       \    Dec 2013
 FB Mathematik der Universitaet, D-67653 Kaiserslautern          \
> ring R = 0,(x,y),lp;
> ideal I = x^4 - y^2 + x^5;
> LIB "normal.lib";
> list nor = normal(I,"var1");
> nor[2];
  [1]:
     _[1] = y
     _[2] = x2
```

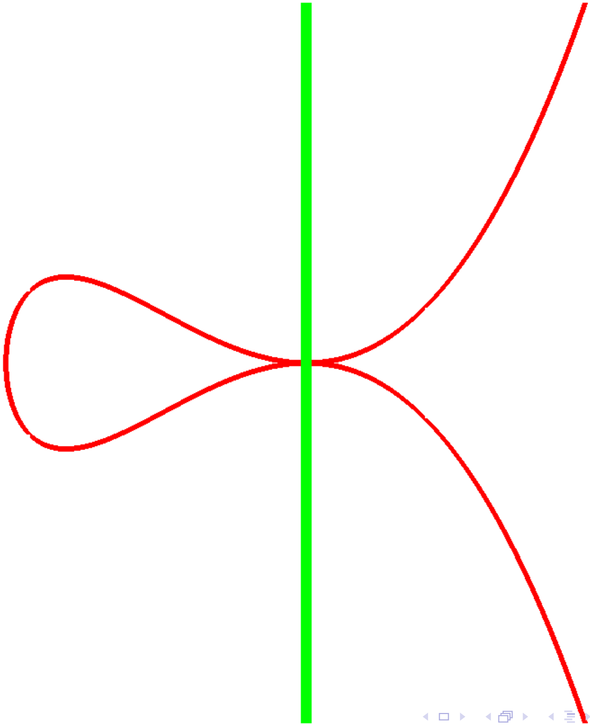
Desingularization of Curves by Normalization

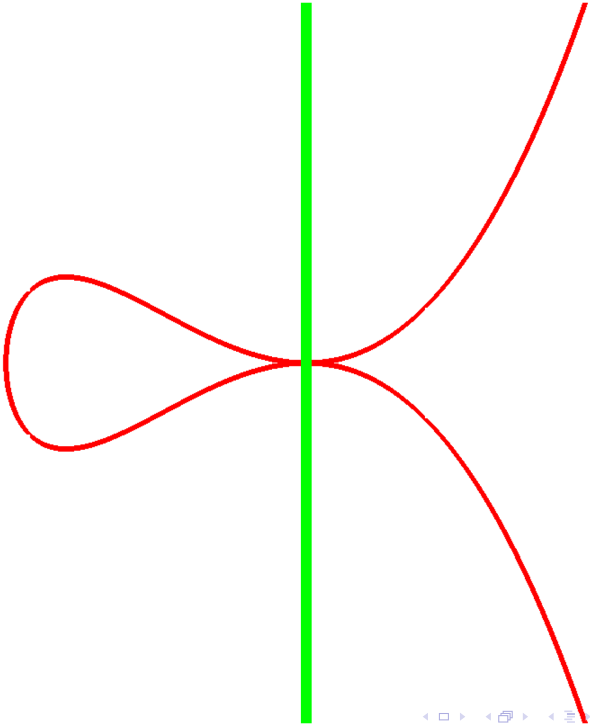
$$C = V(x^4 - y^2 + x^5)$$
$$t = \frac{y}{x^2}$$

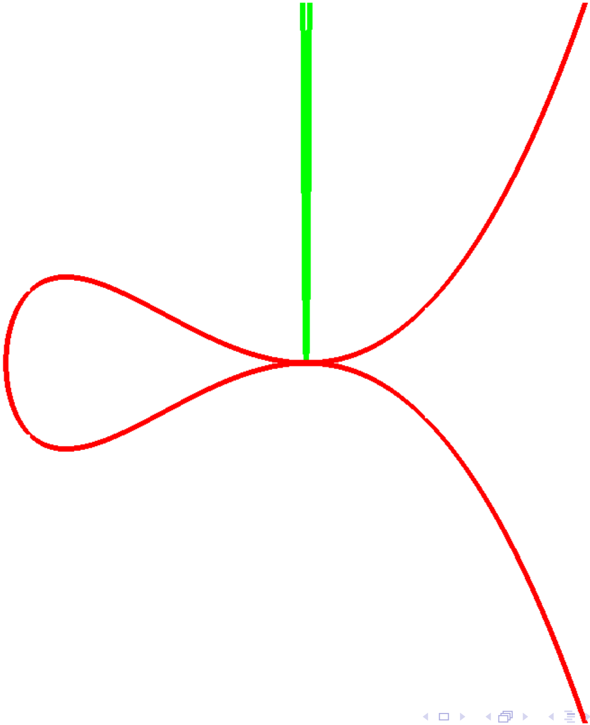
Desingularization of Curves by Normalization

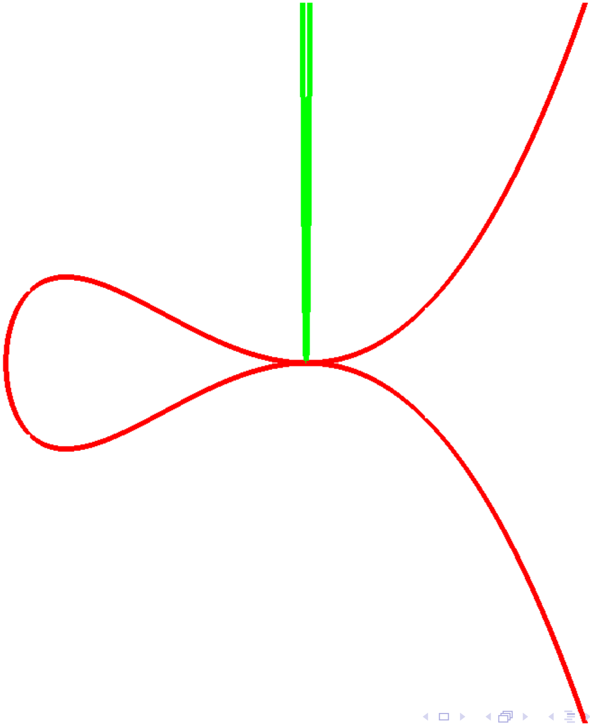
$$C = V(x^4 - y^2 + x^5)$$
$$t = \frac{y}{x^2}$$

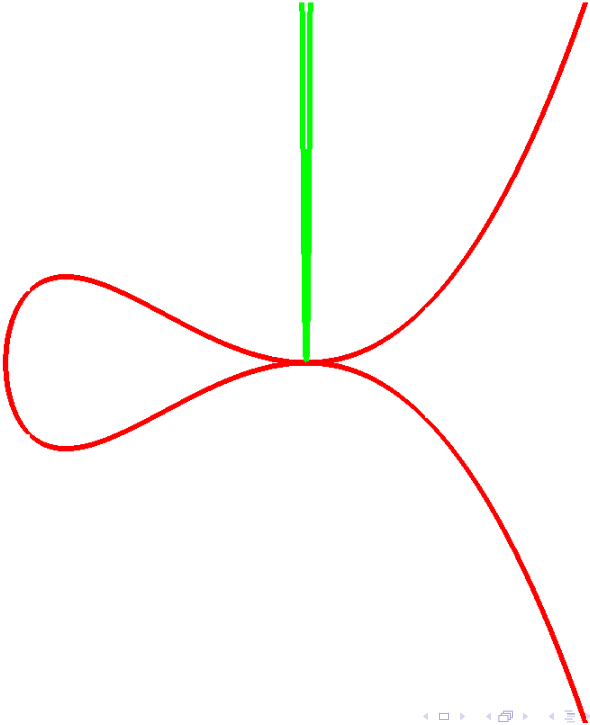


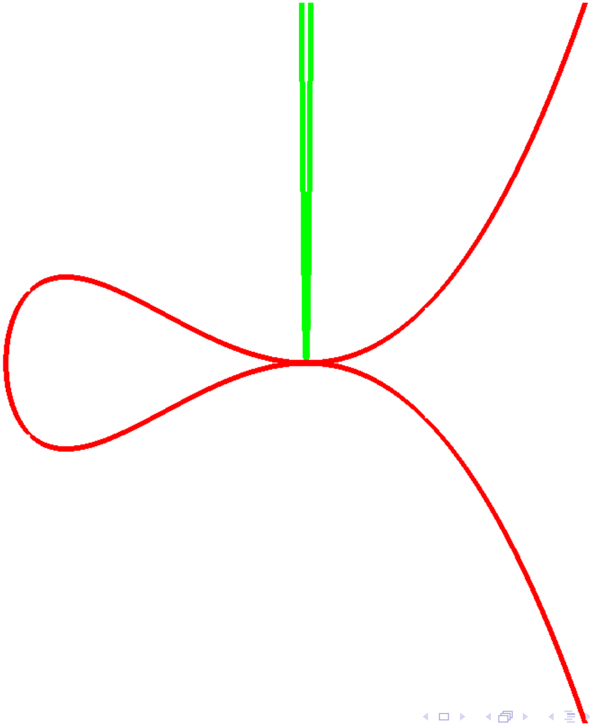


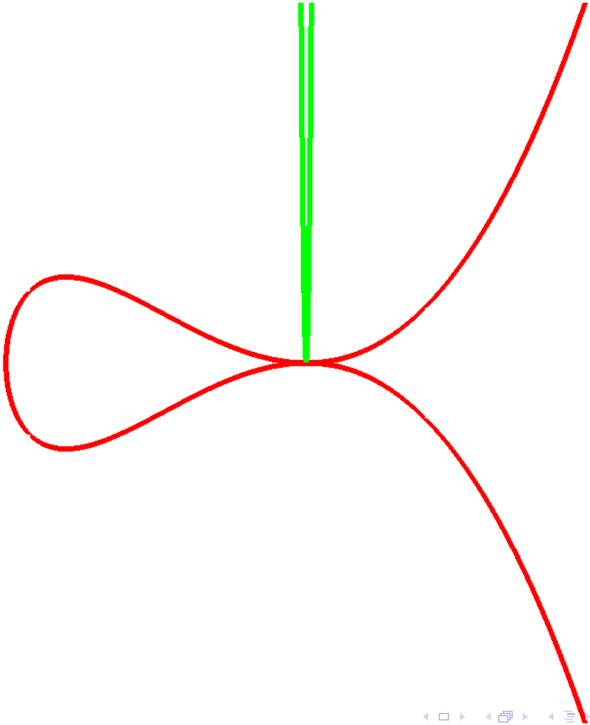


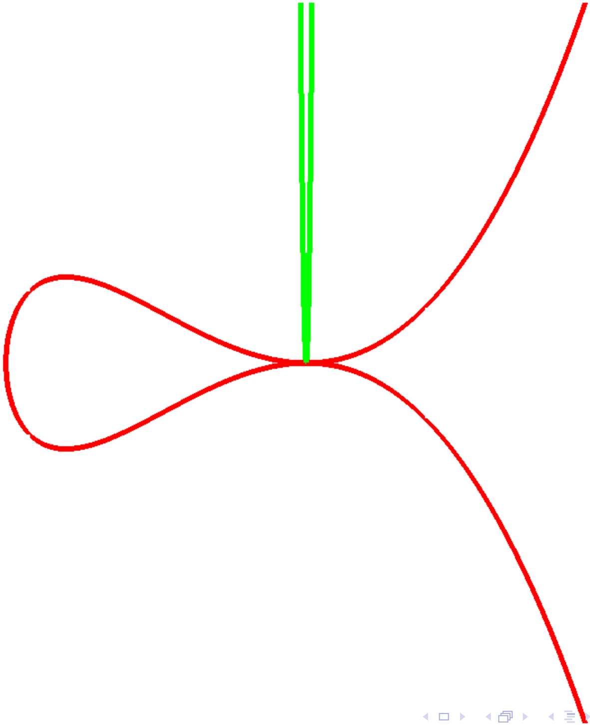


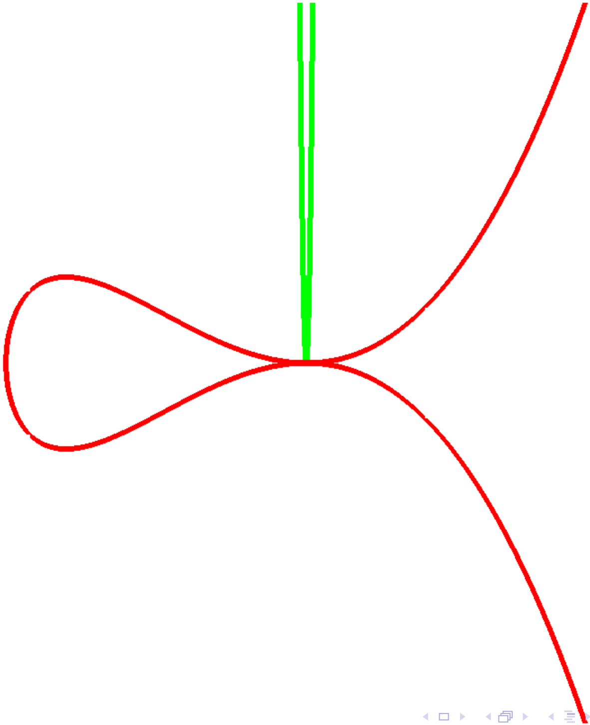


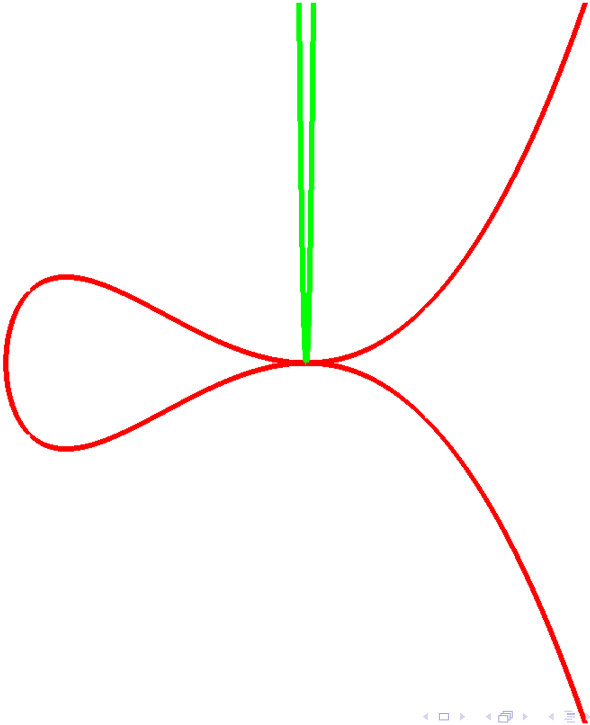


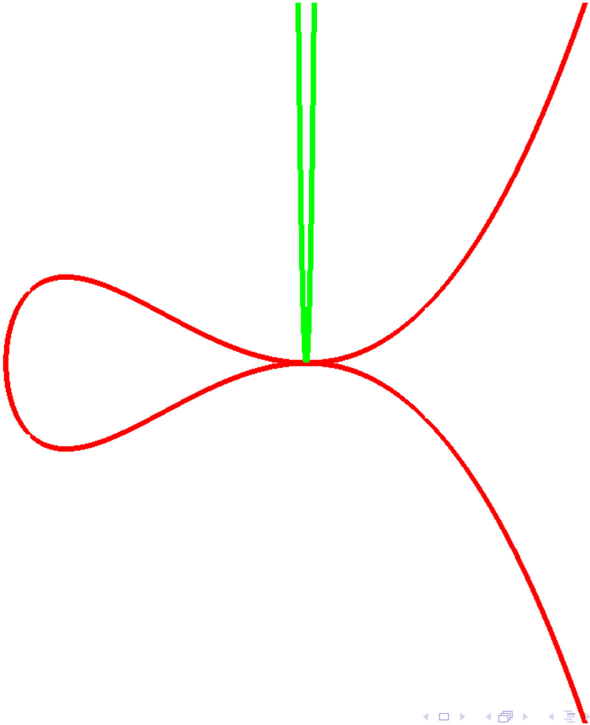


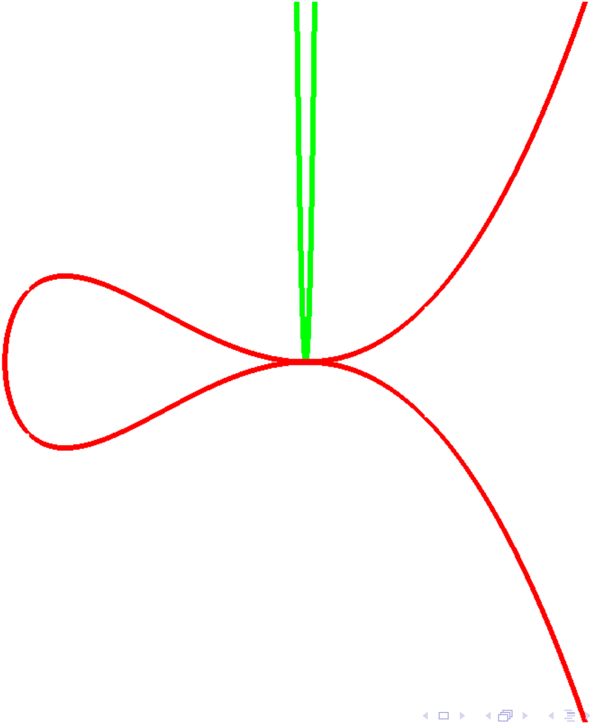


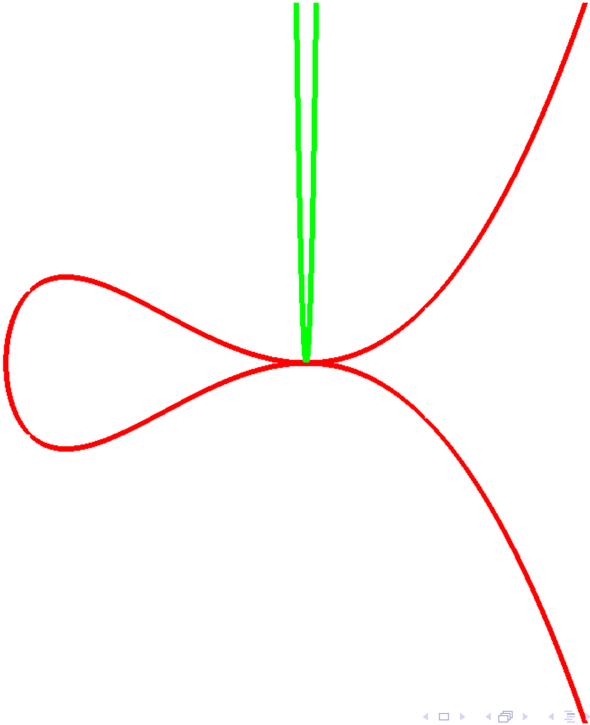


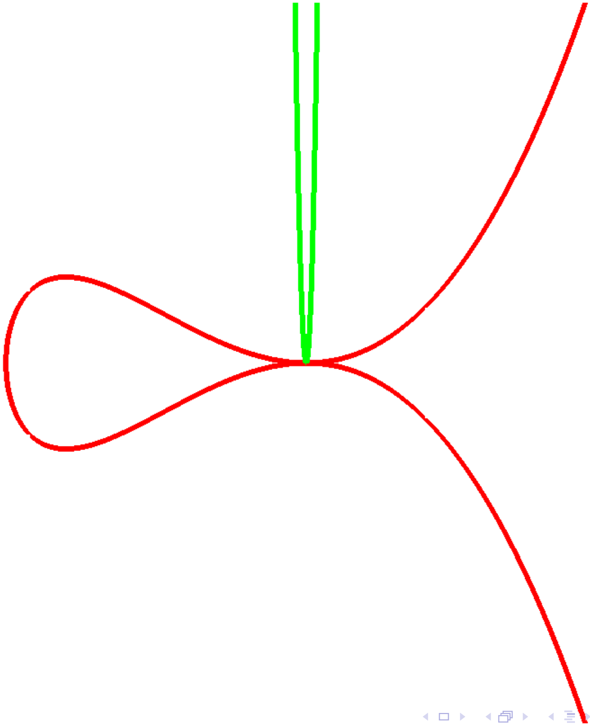


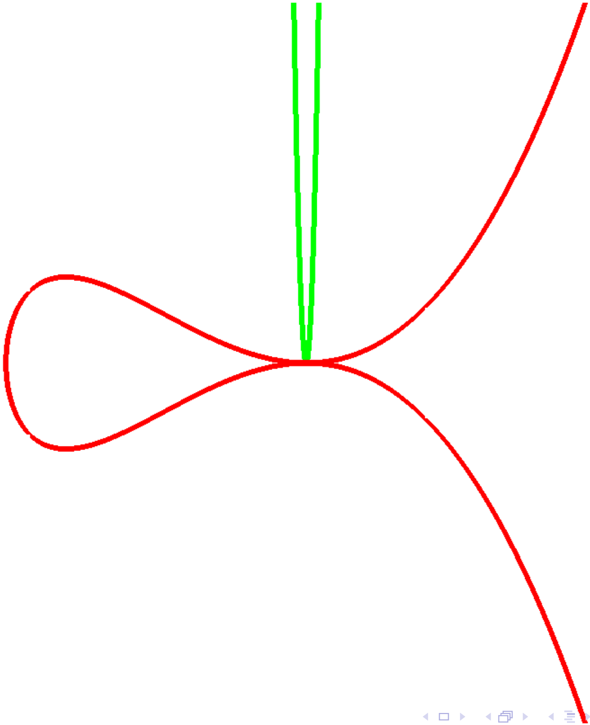


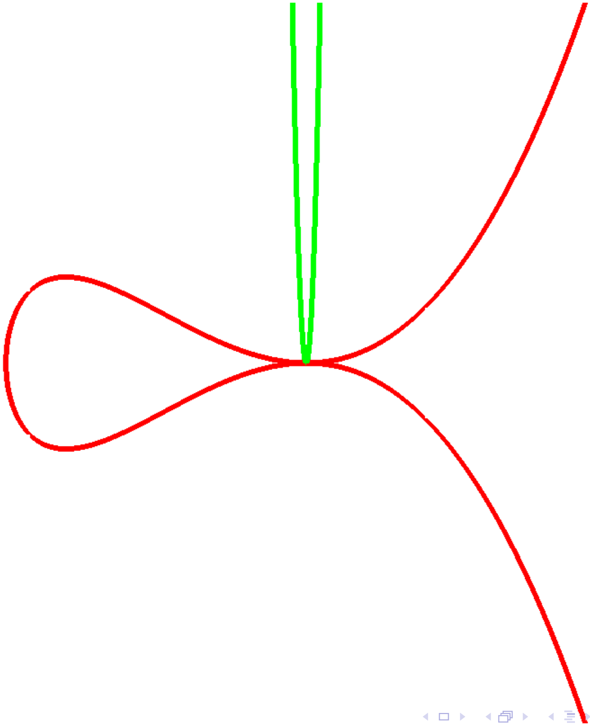


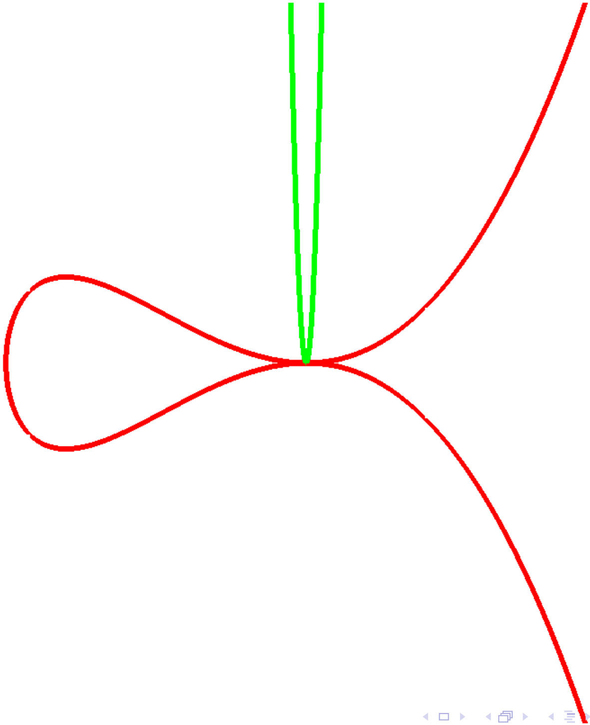


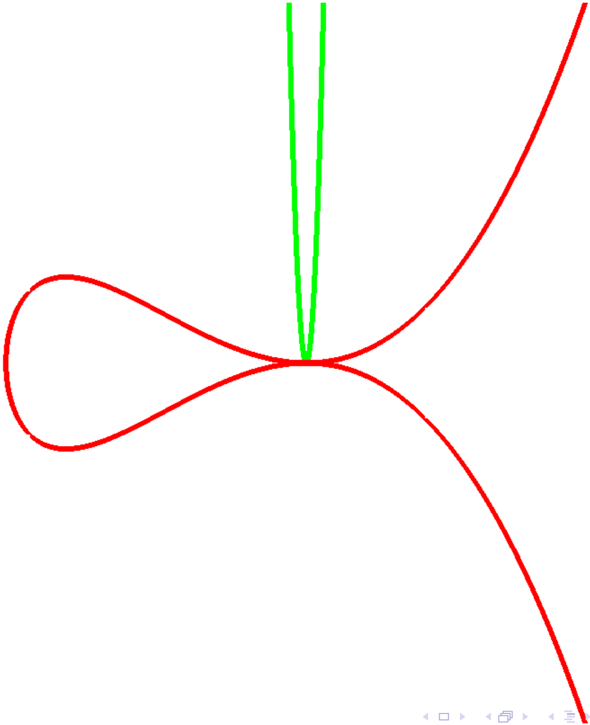


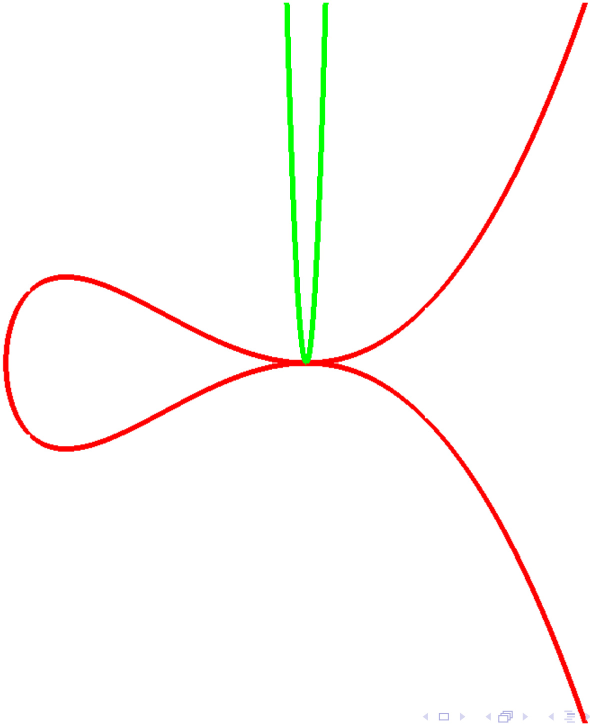


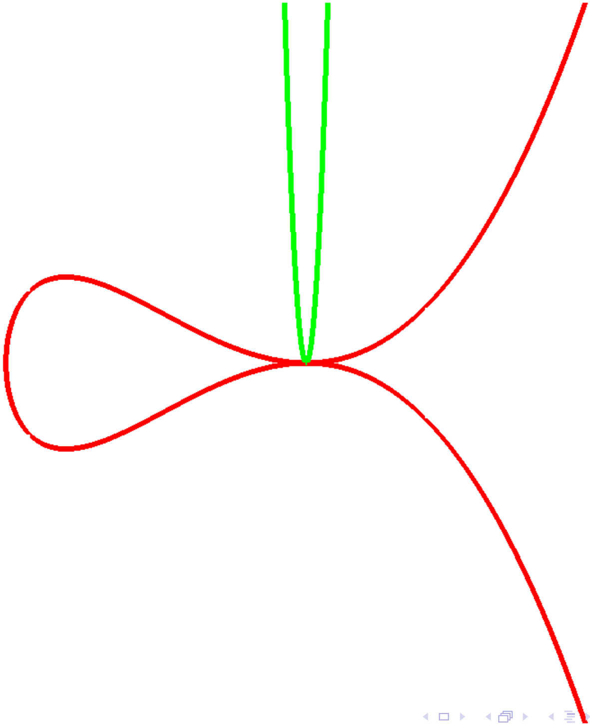


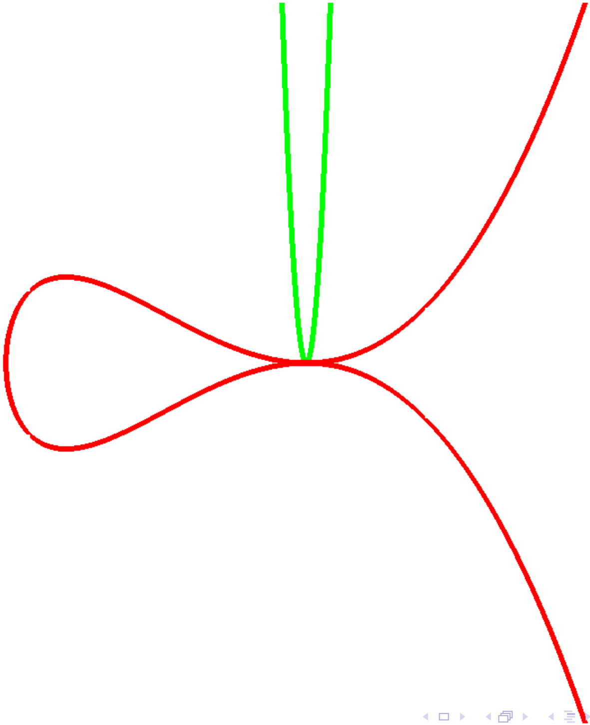


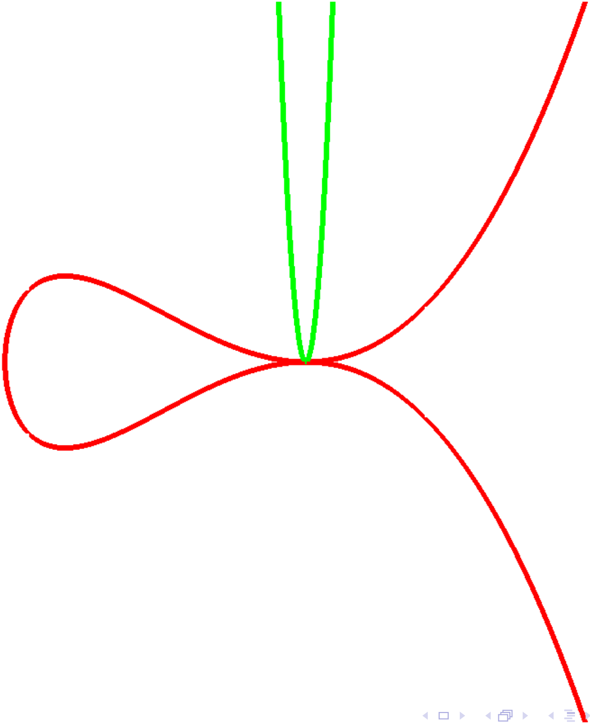


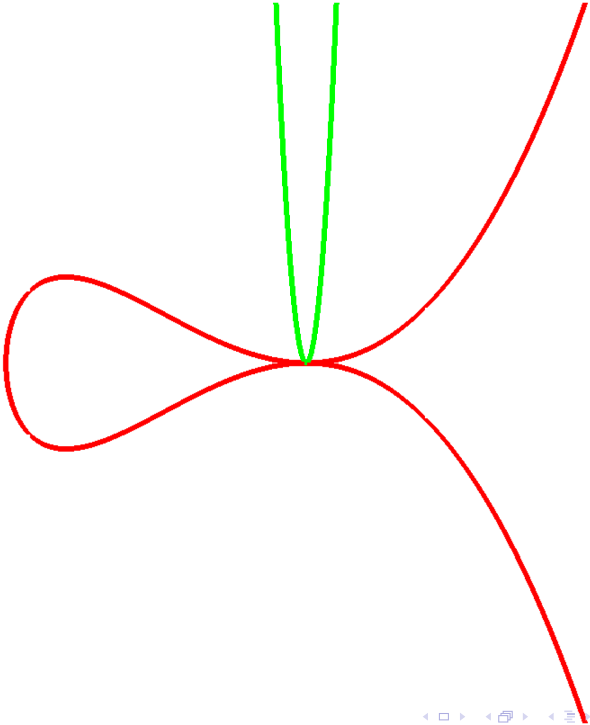


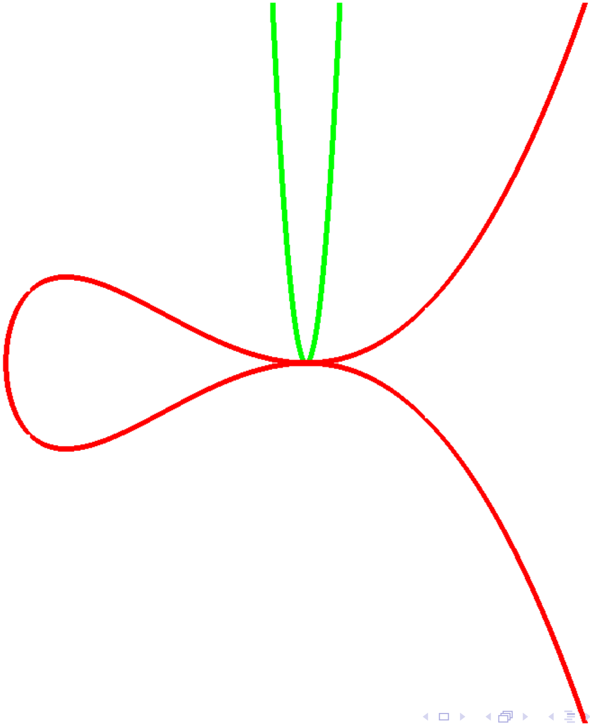


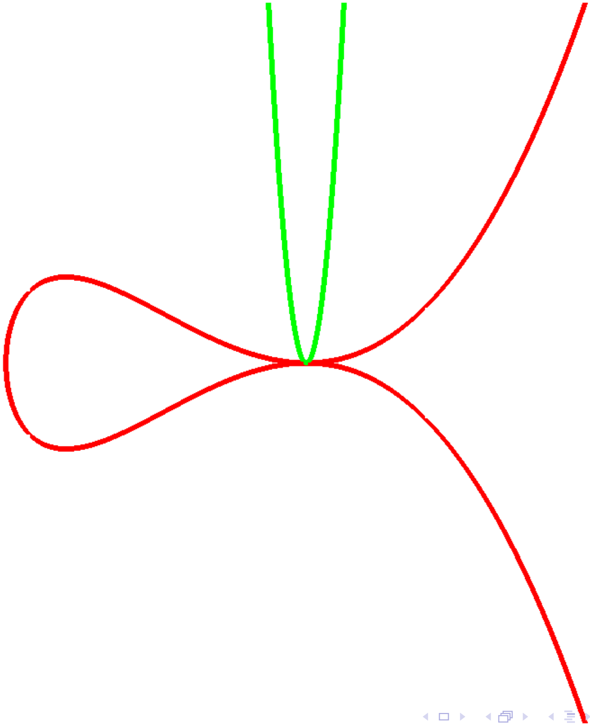


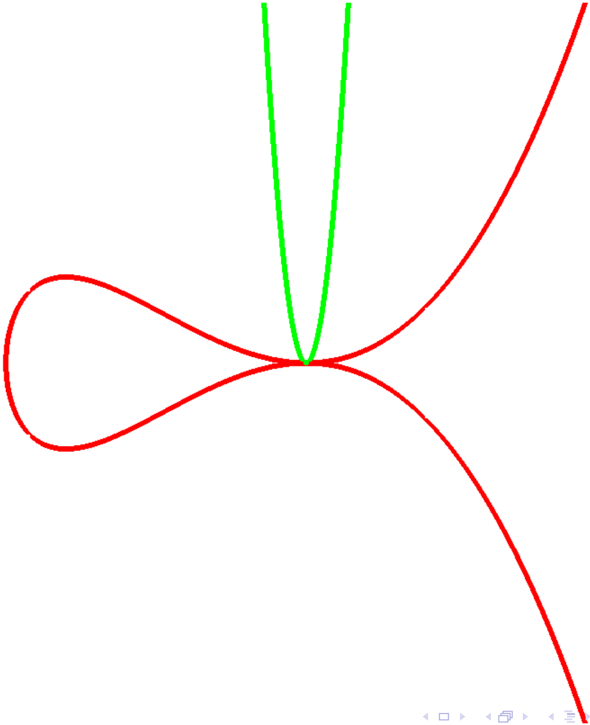


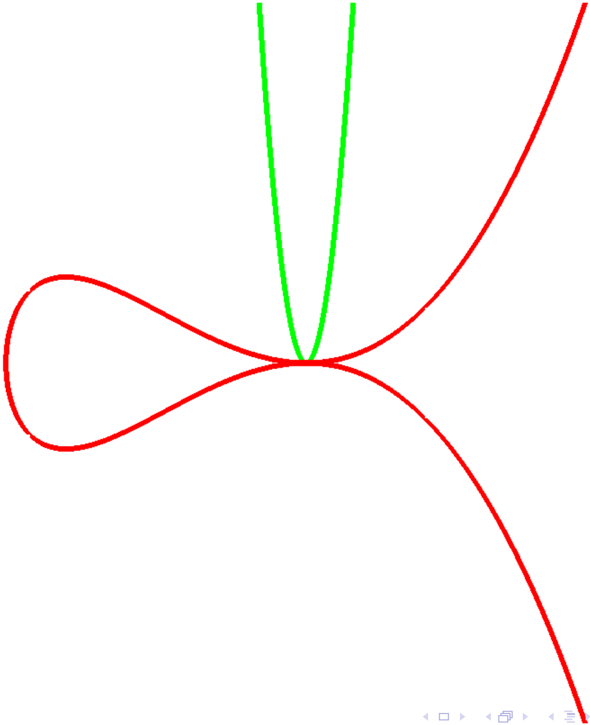


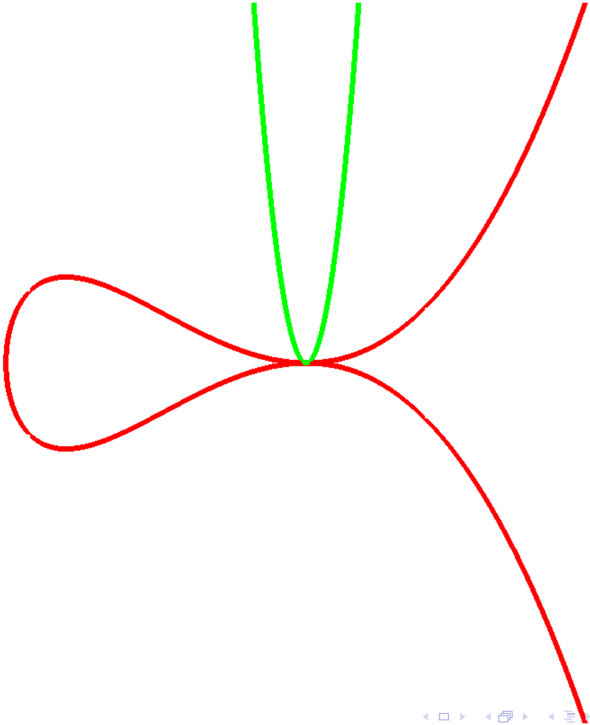


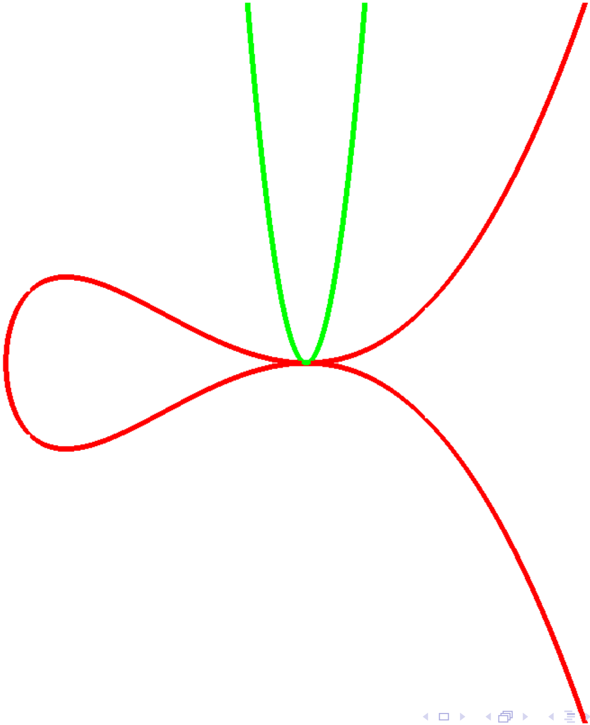


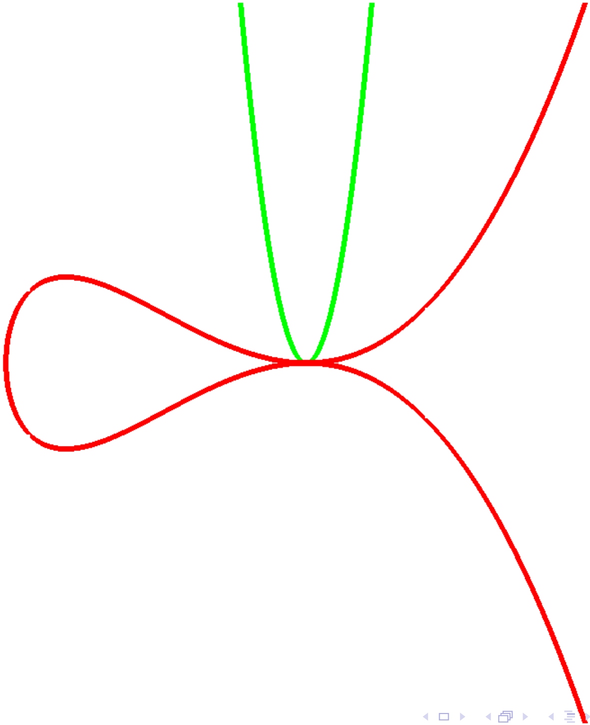


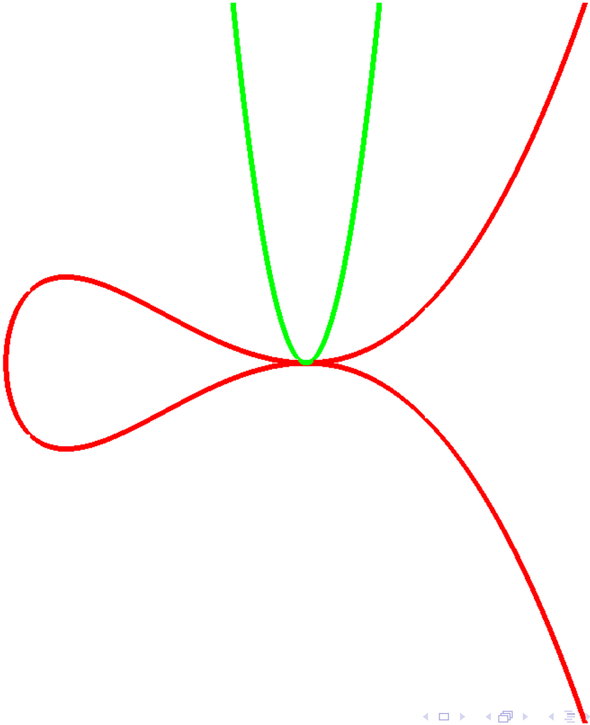


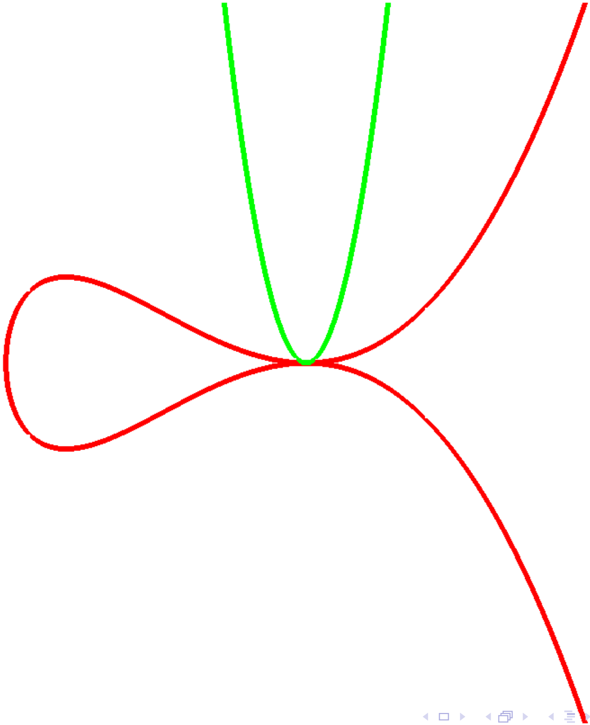


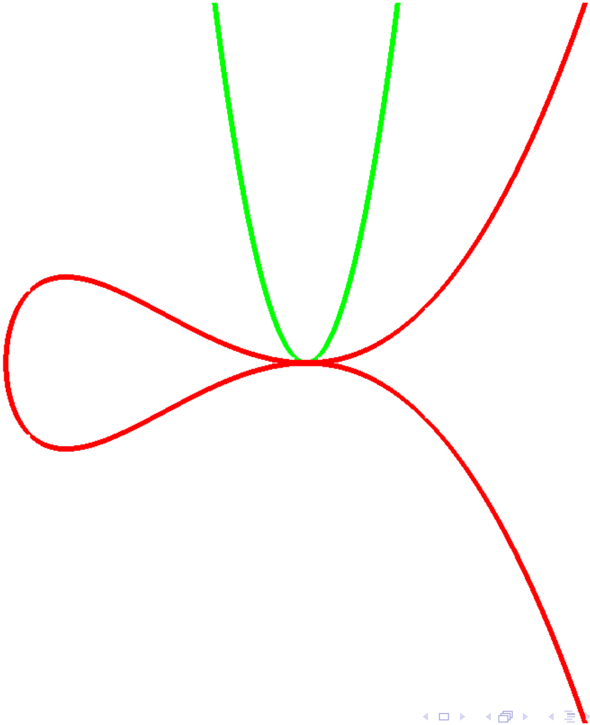


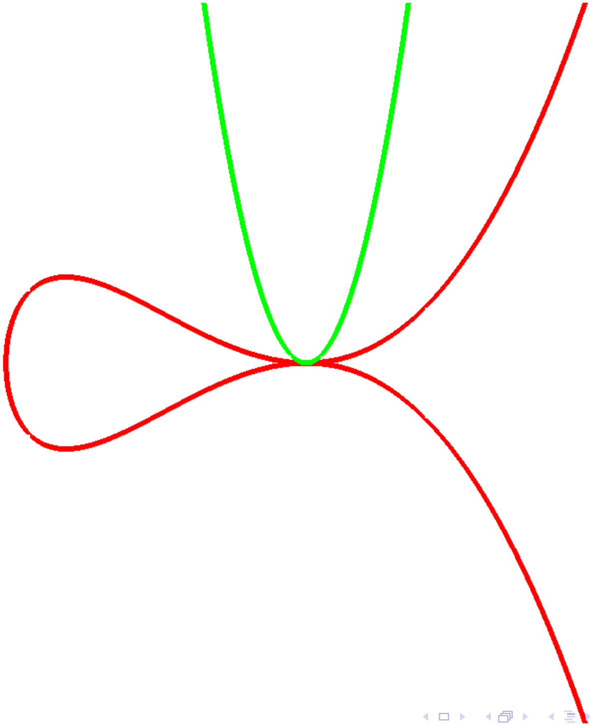


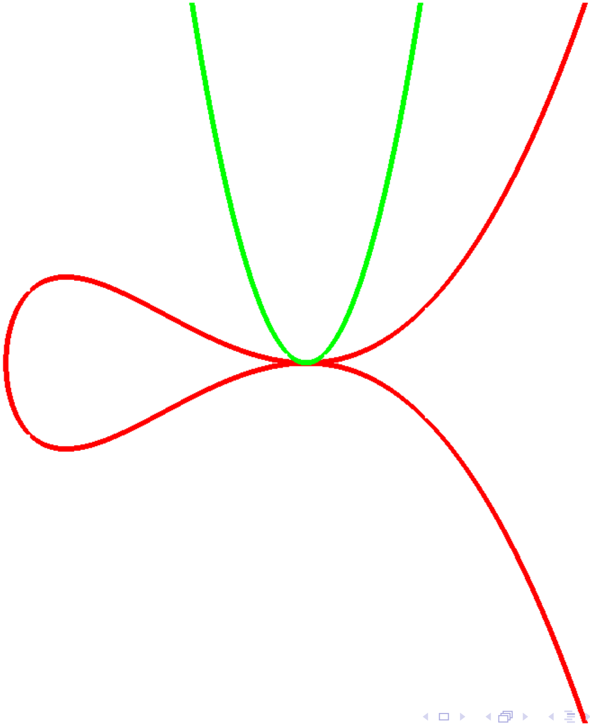


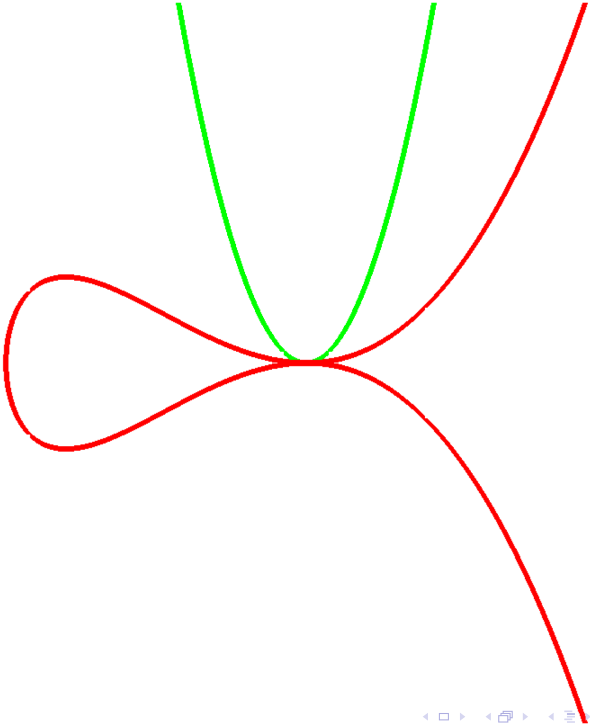


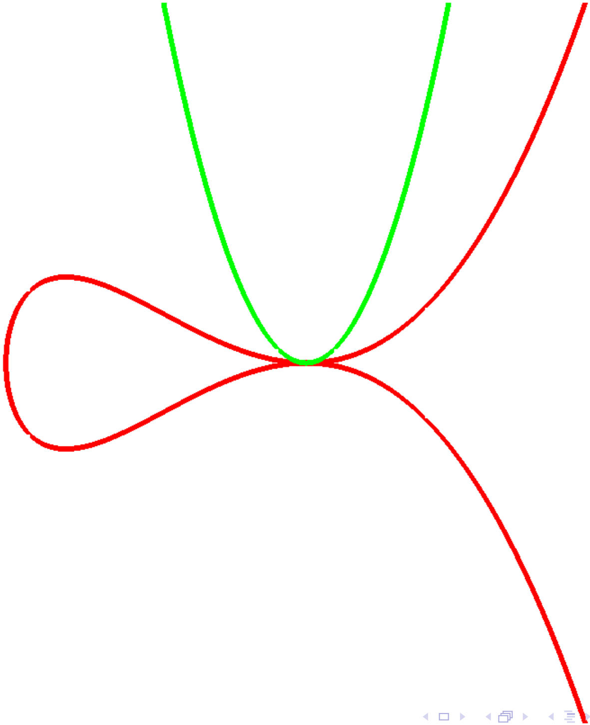


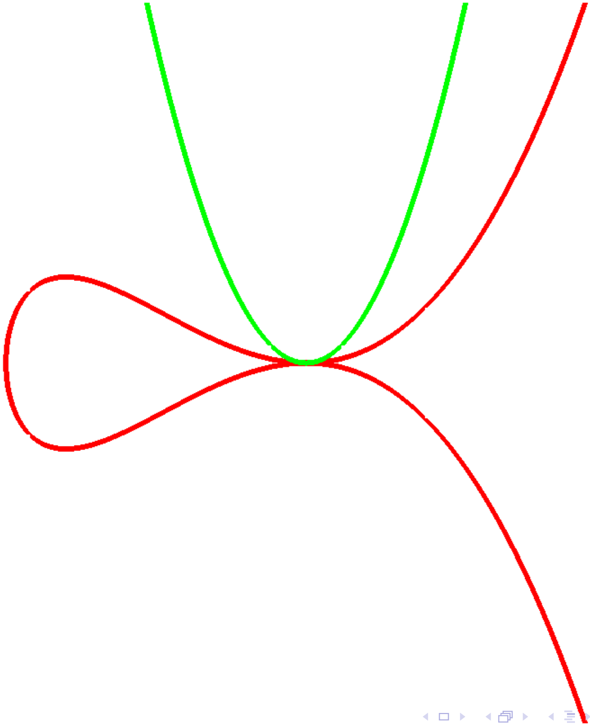


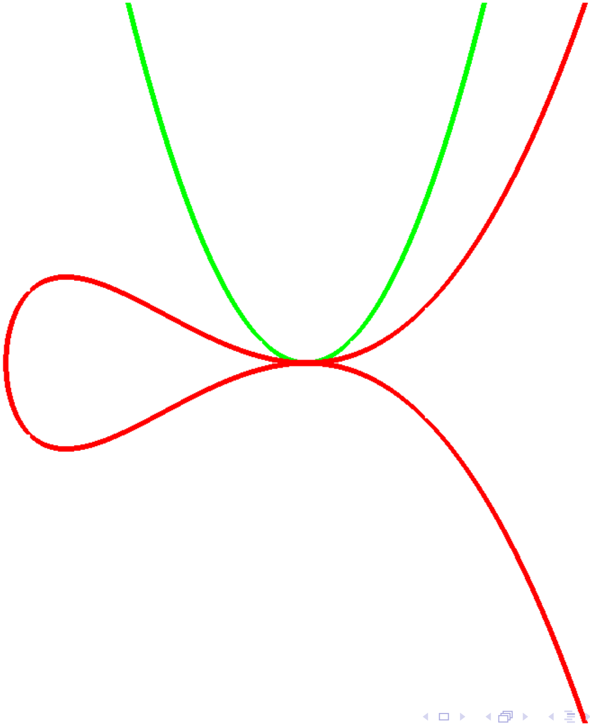


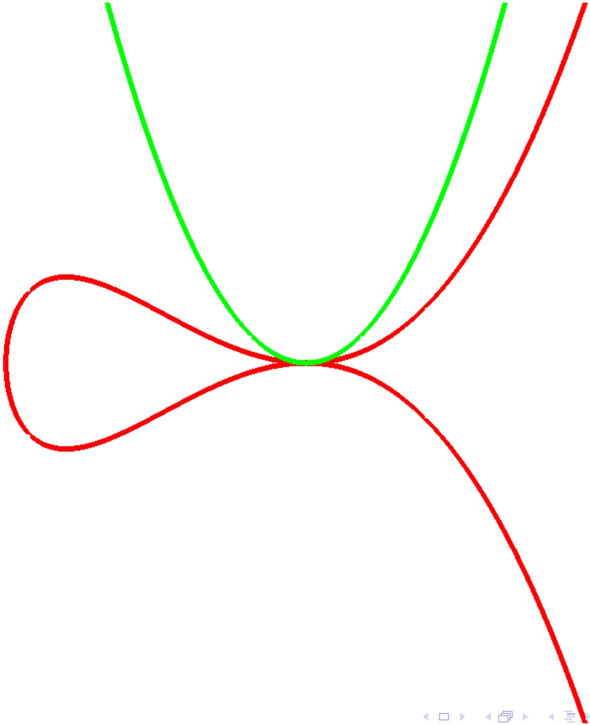


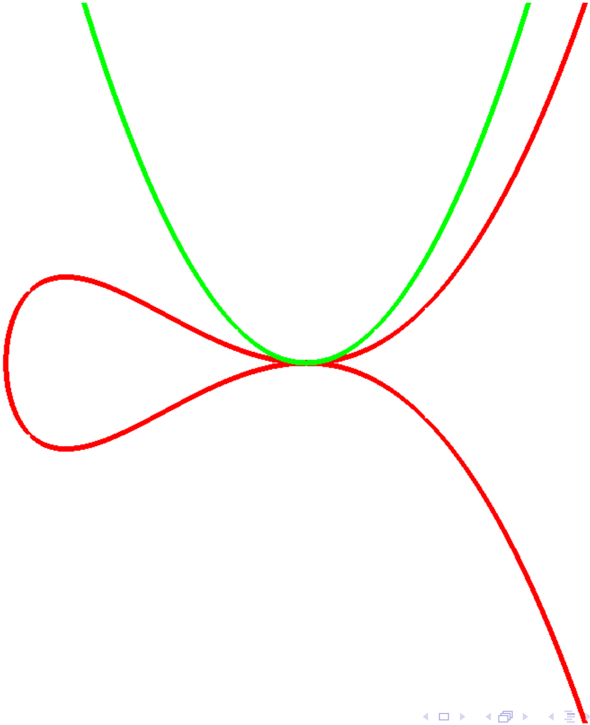


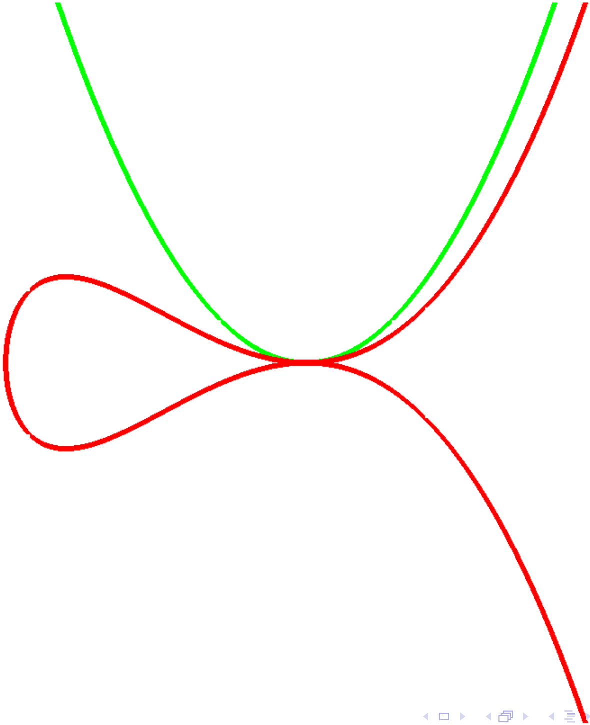


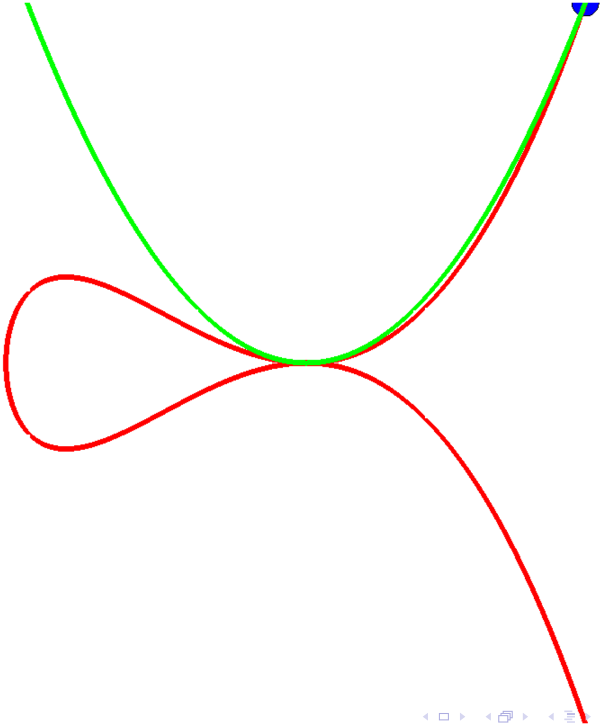


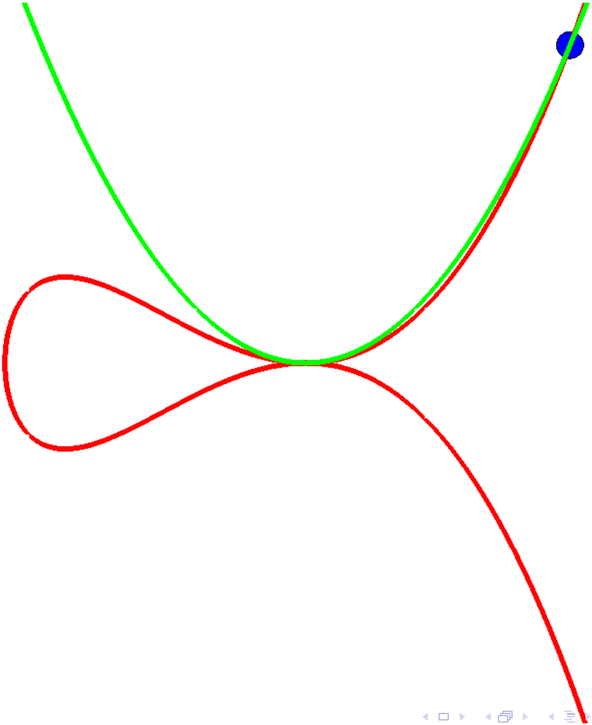


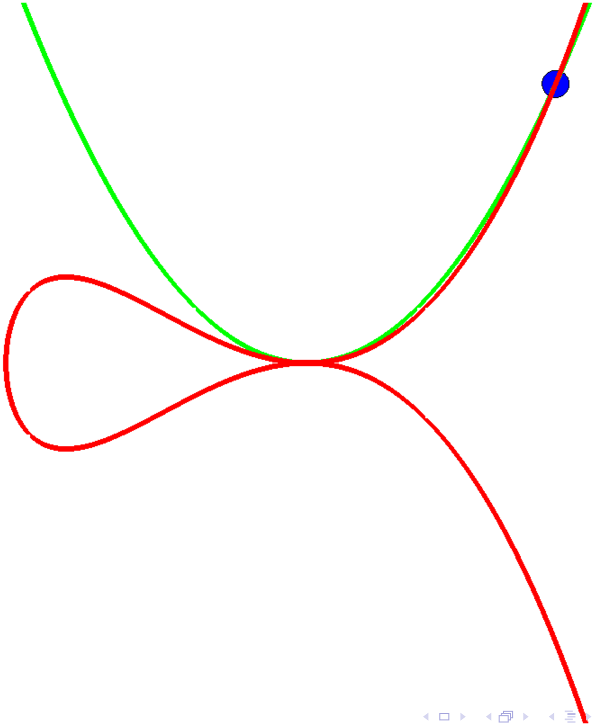


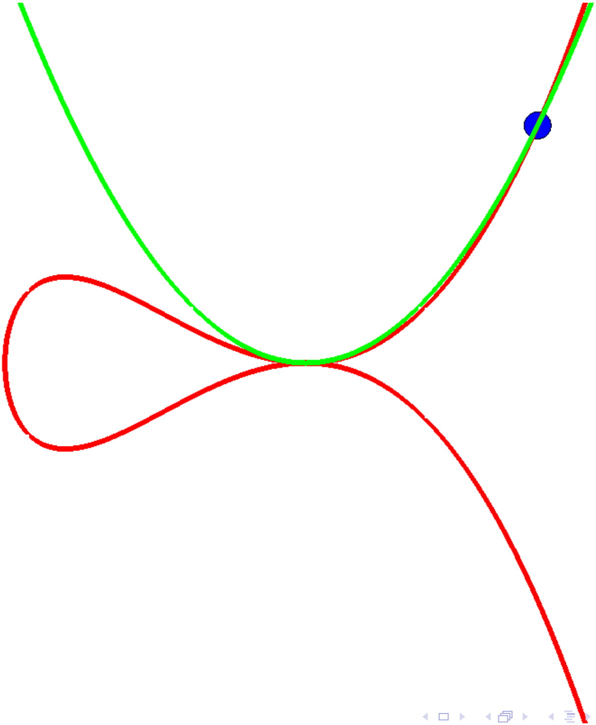


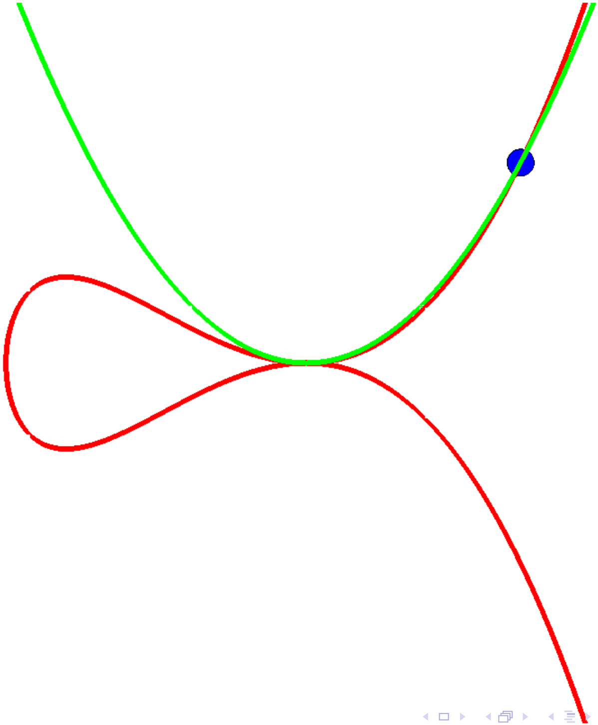


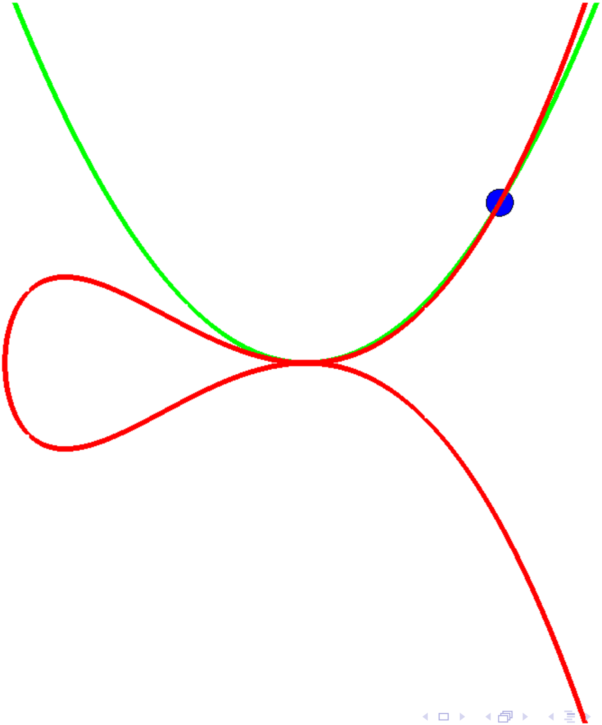


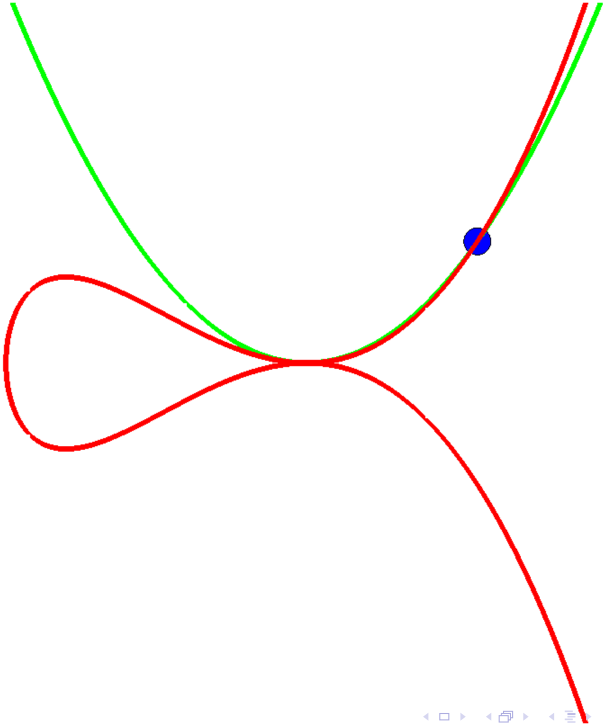


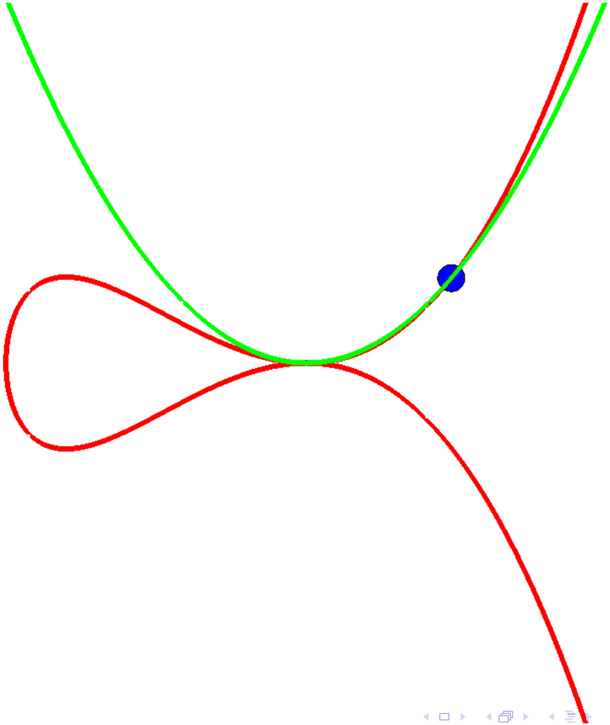


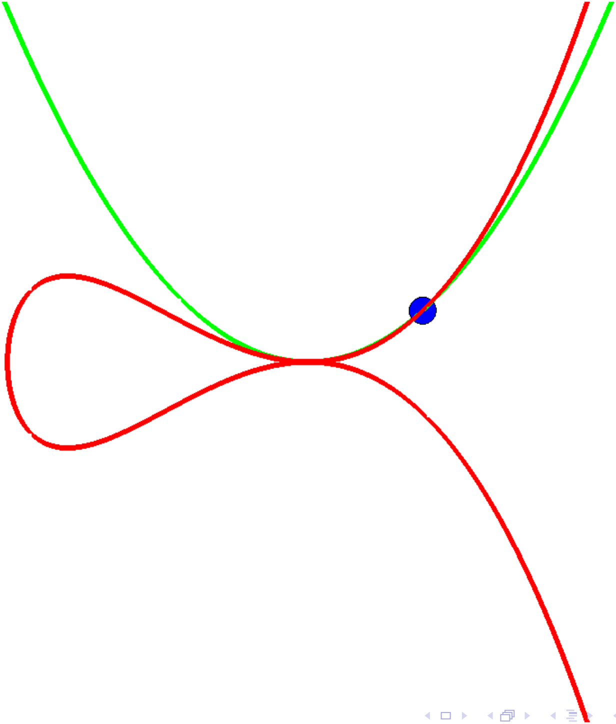


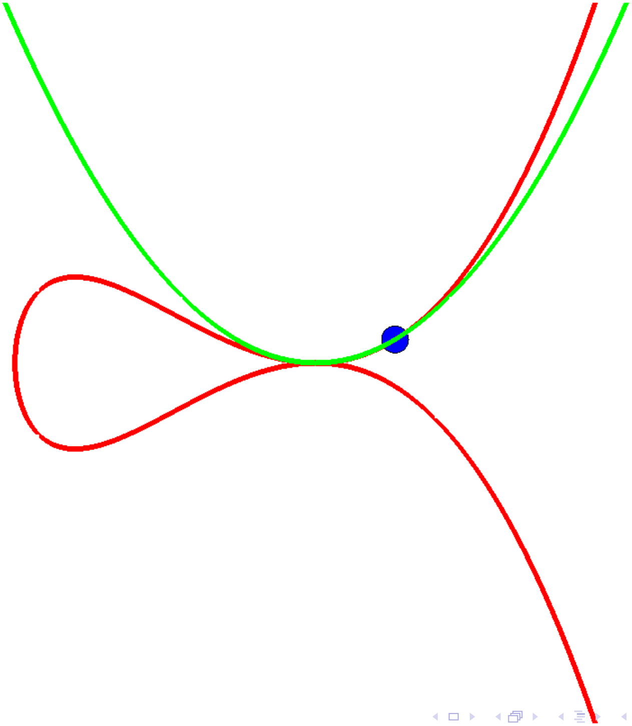


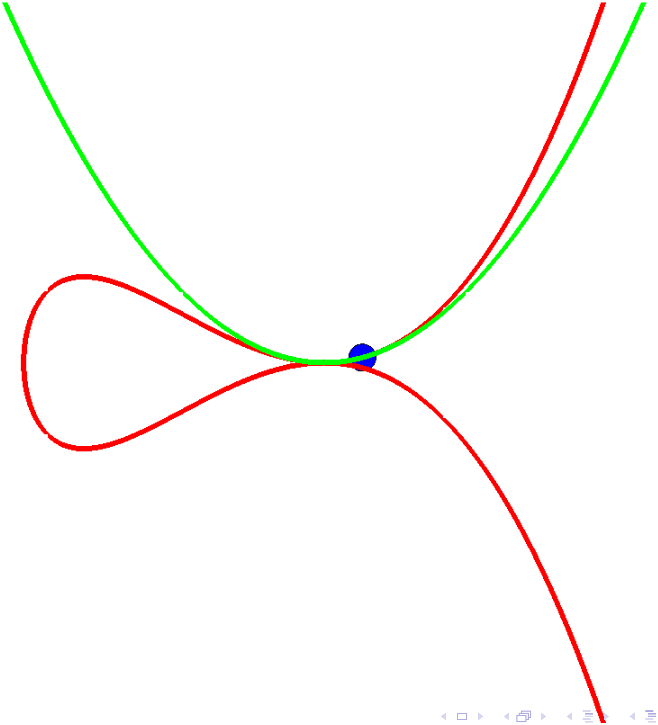


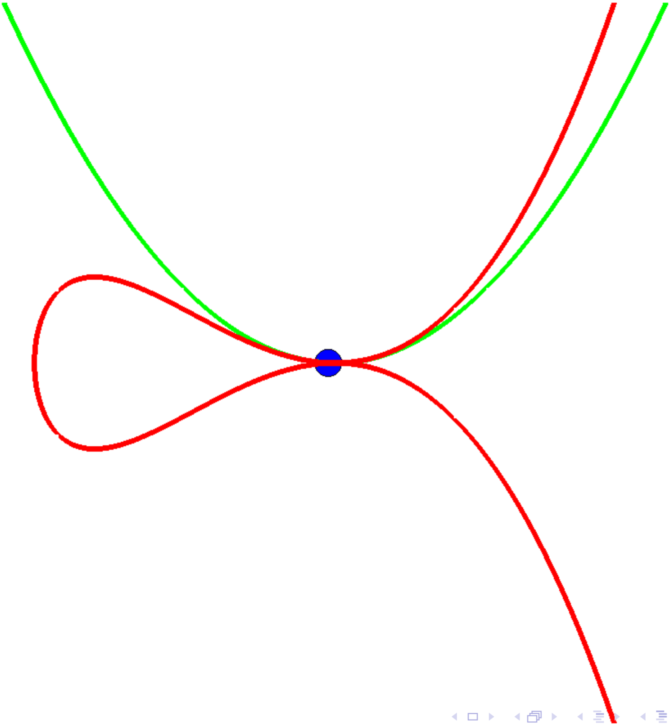


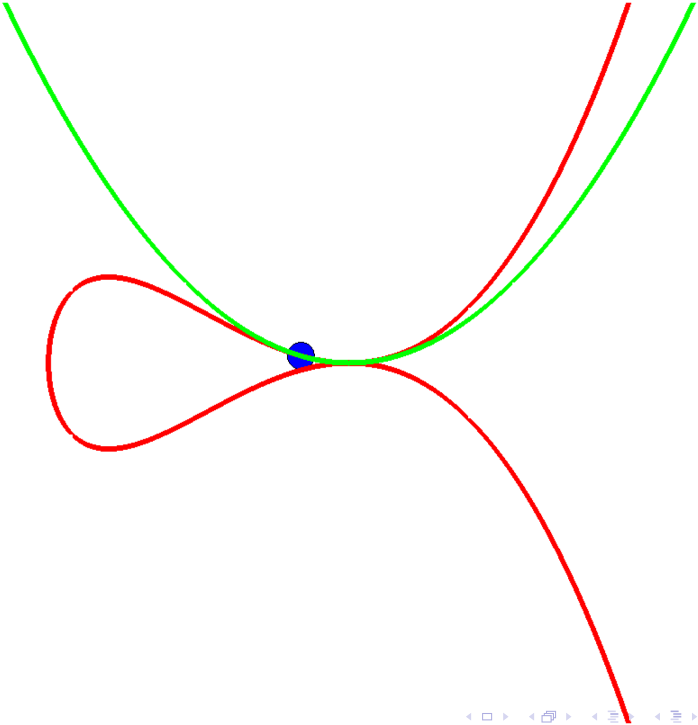


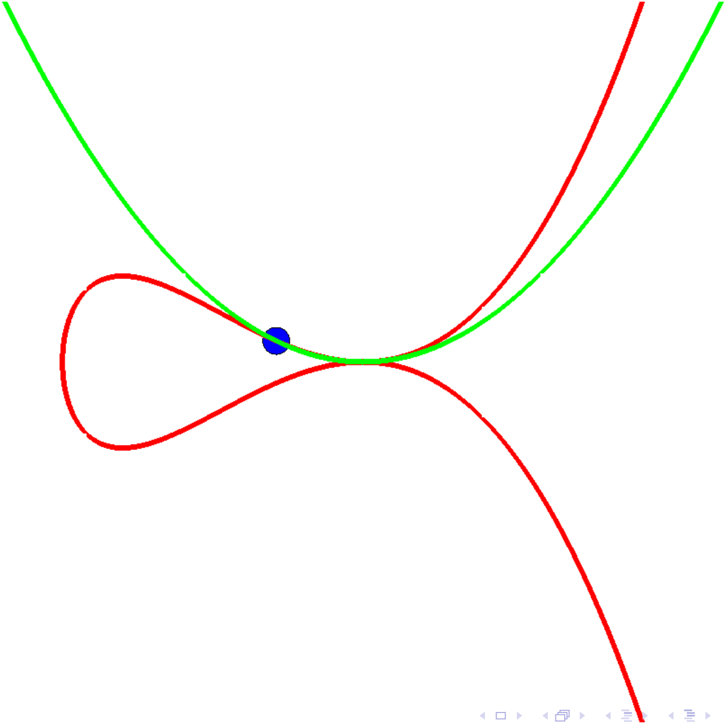


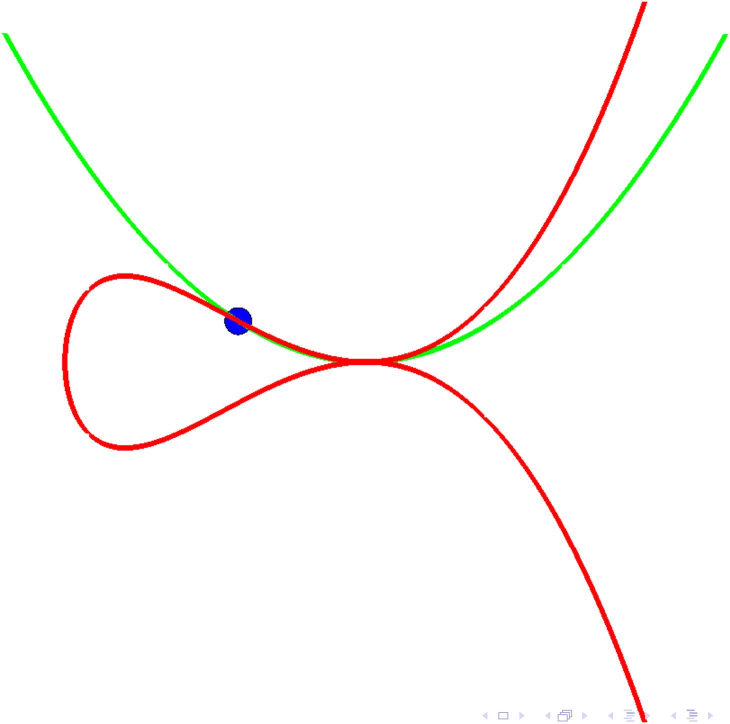


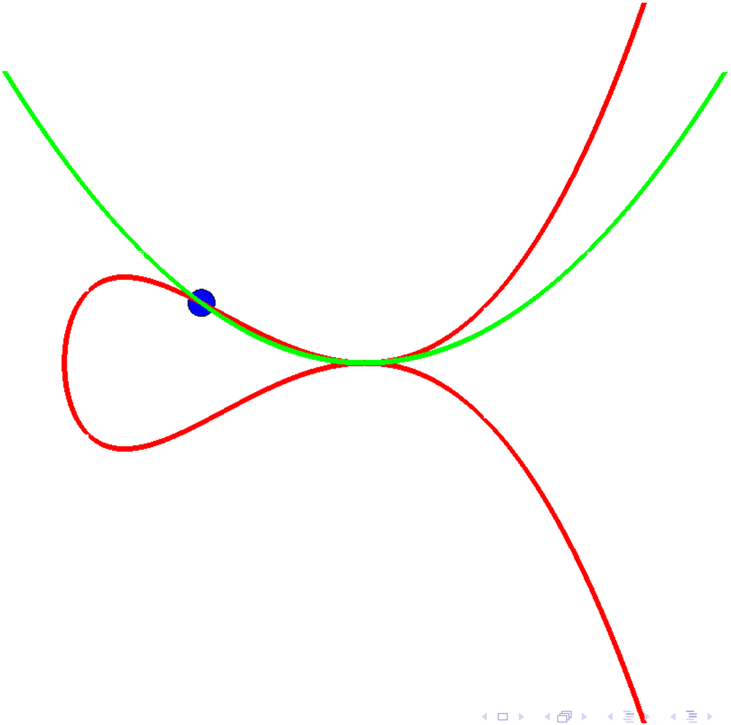


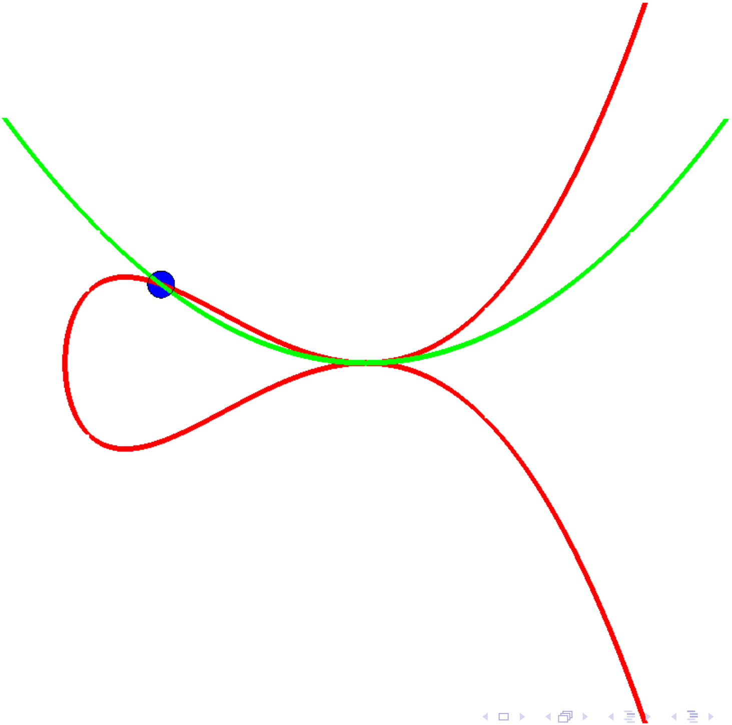


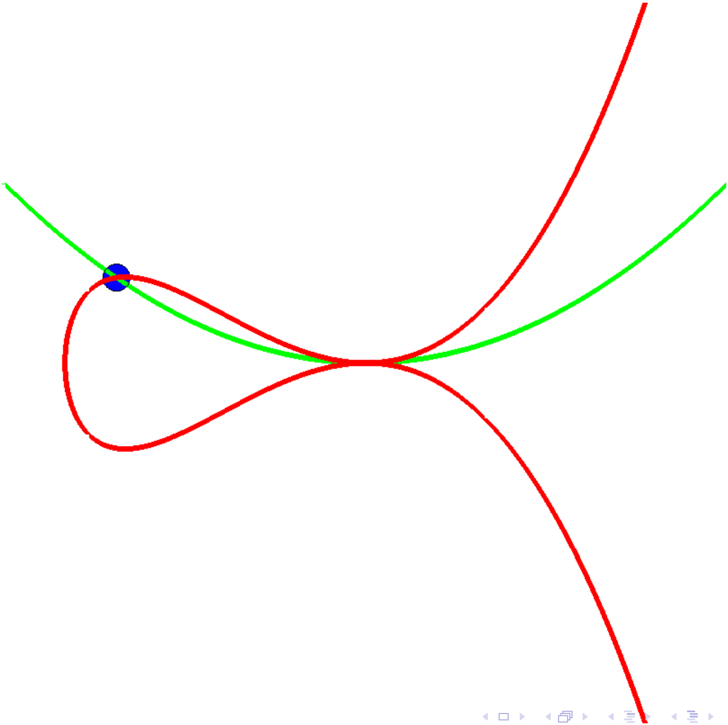


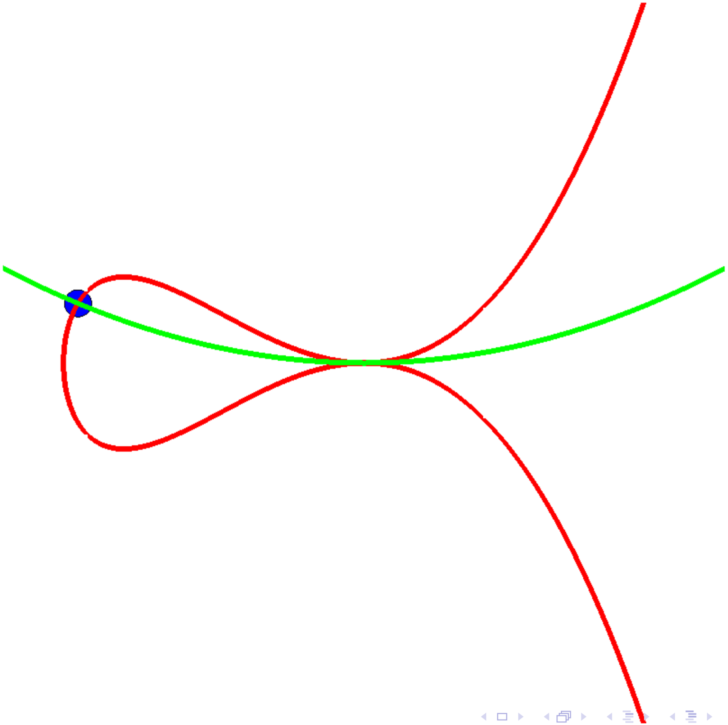


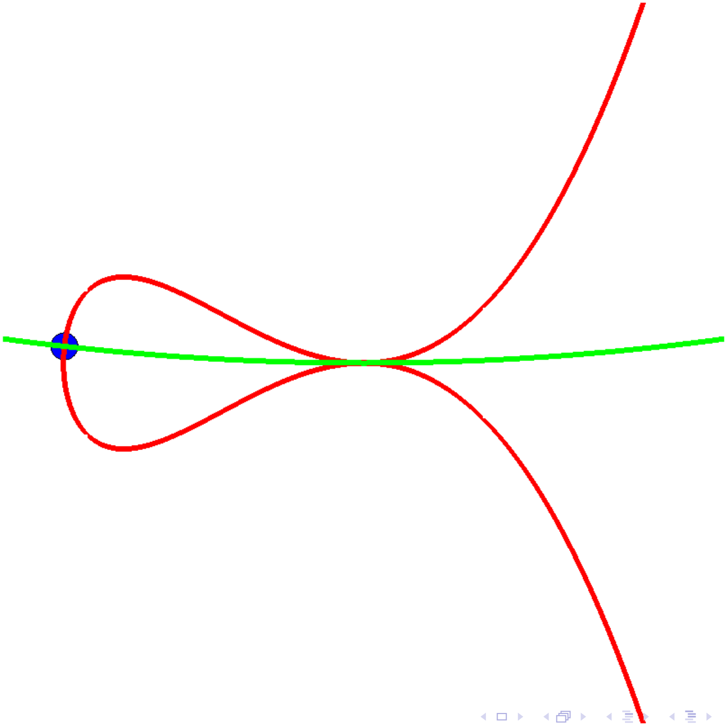


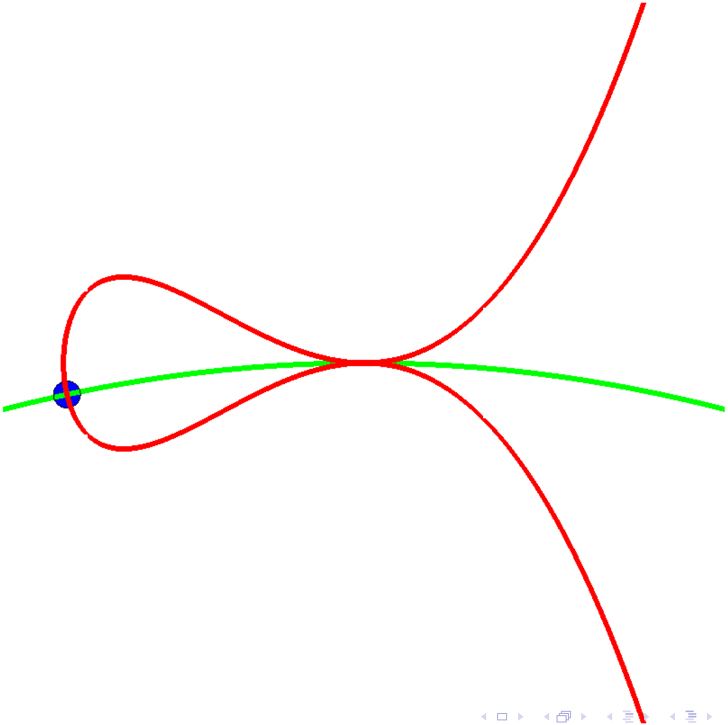


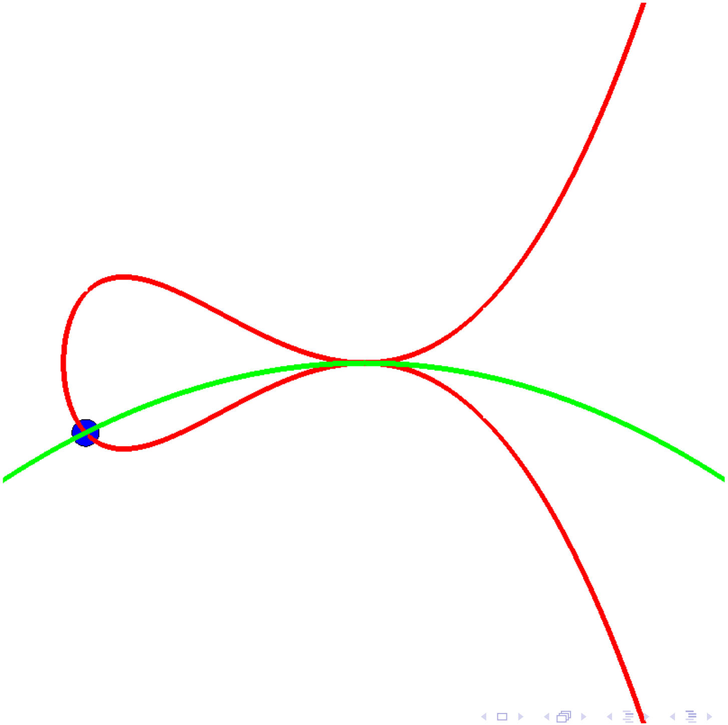


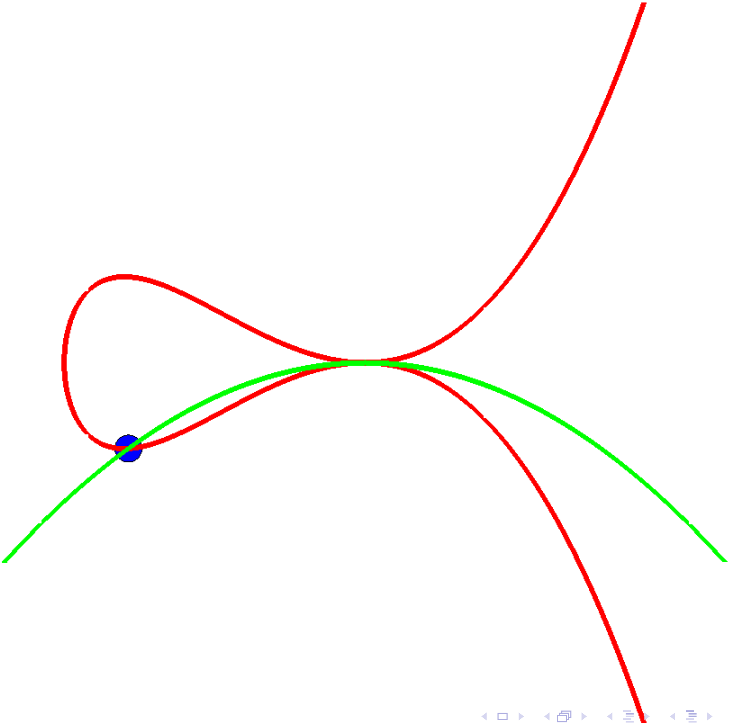


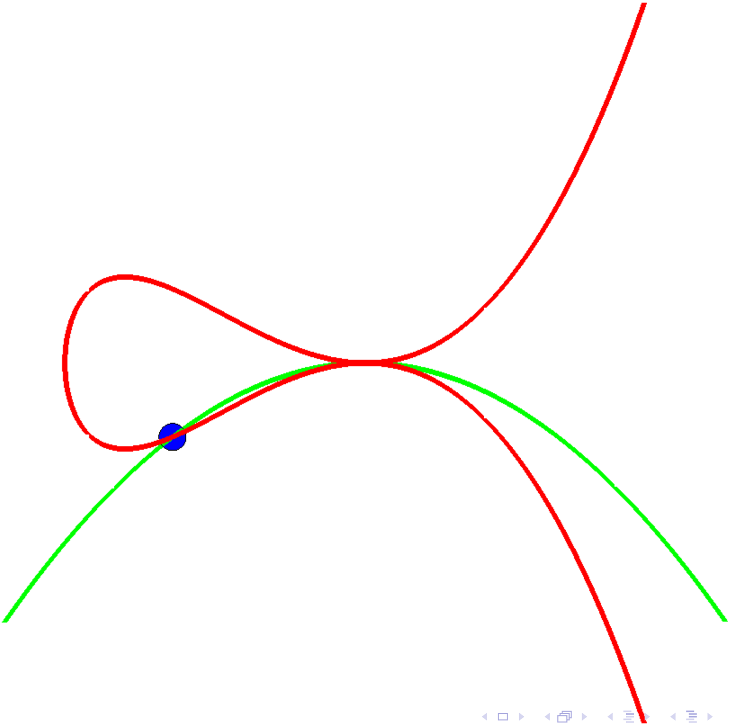


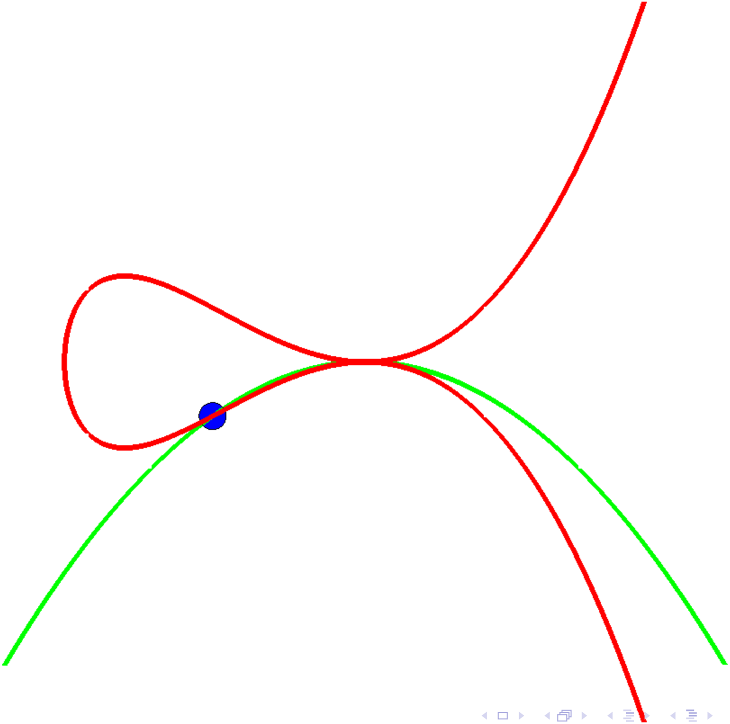


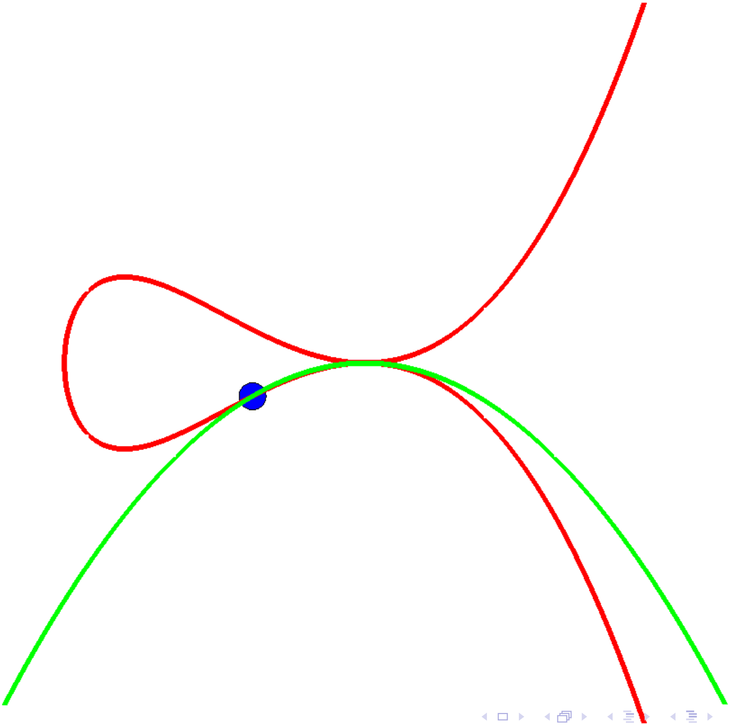


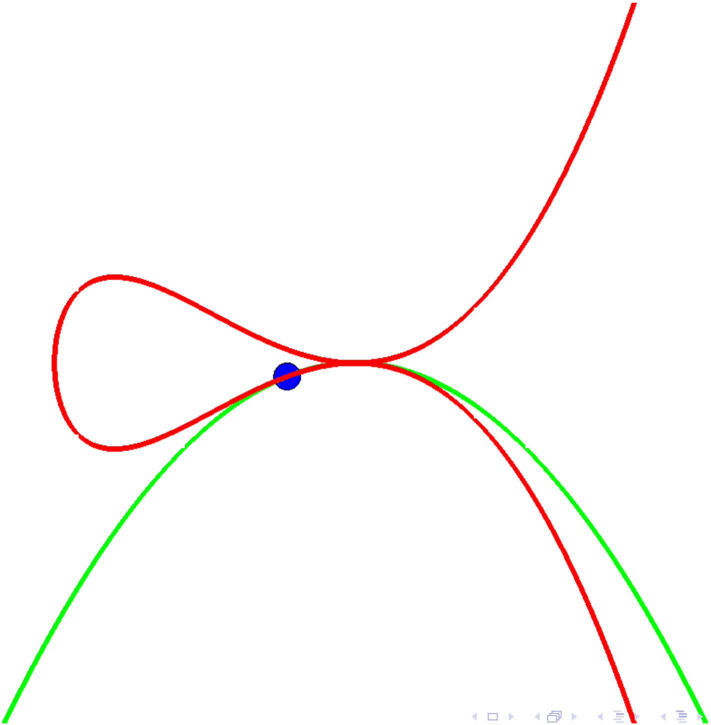


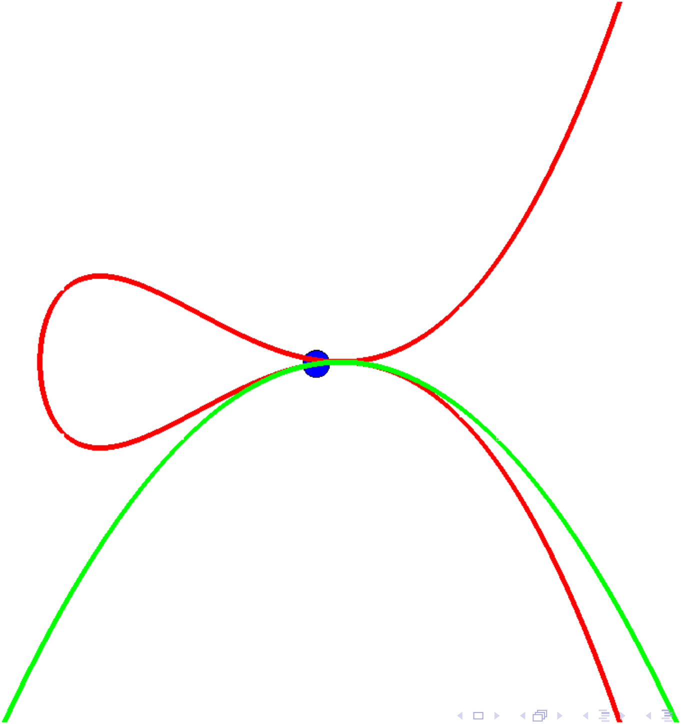


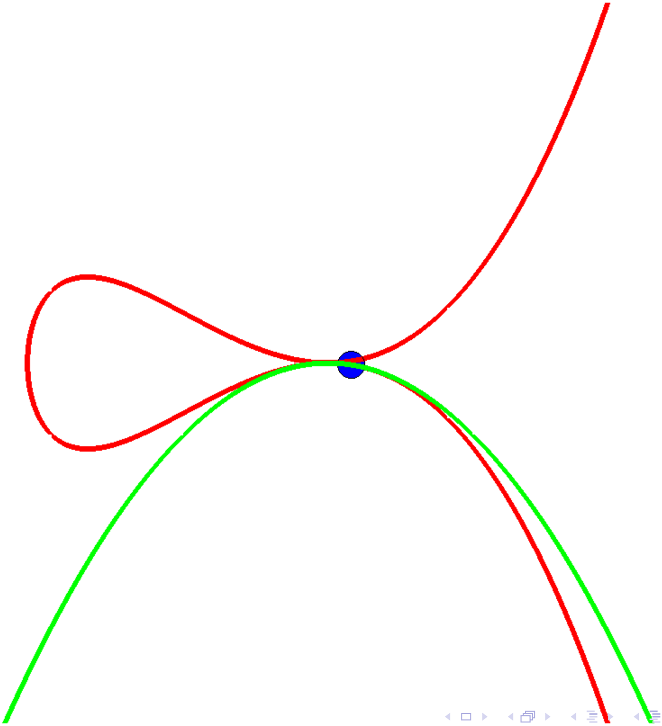


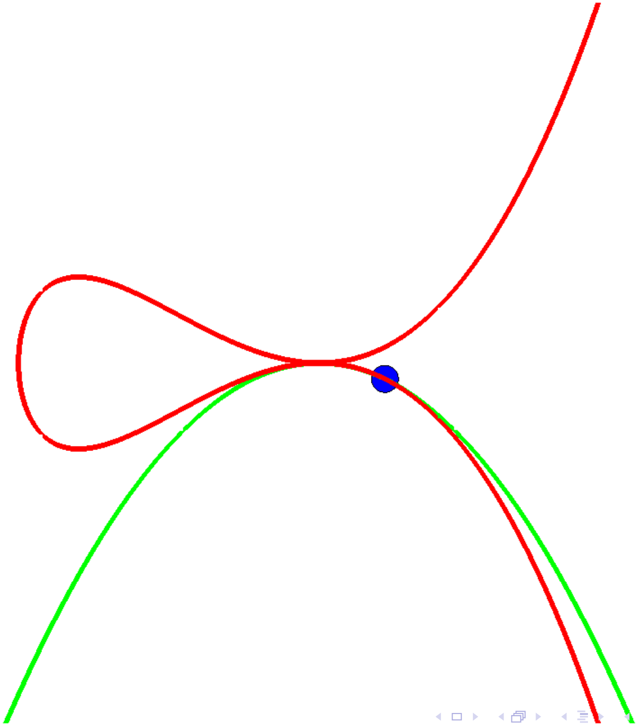


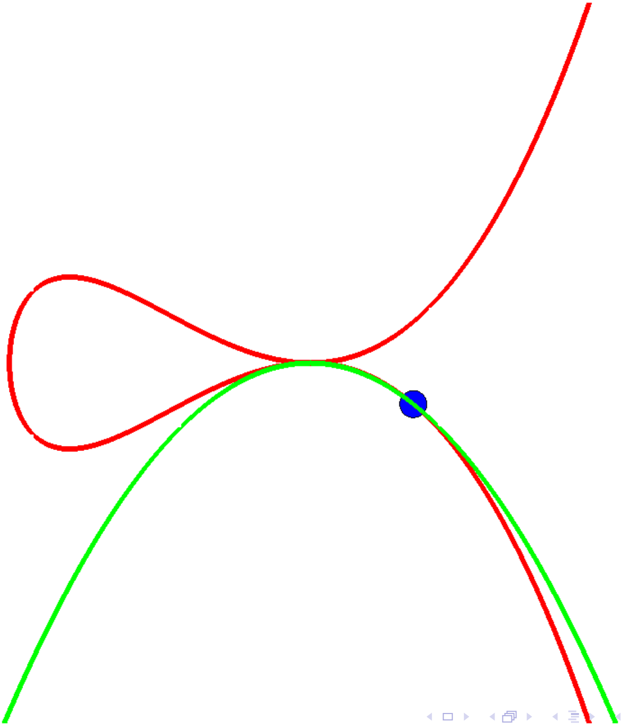


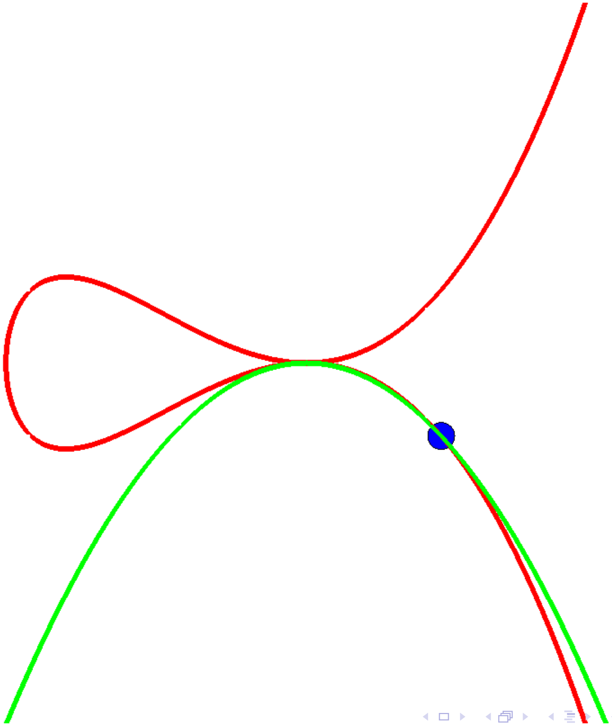


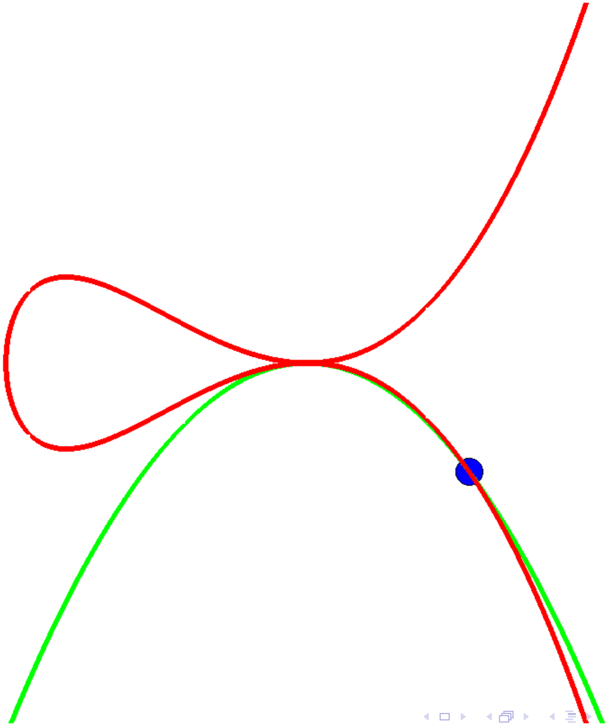


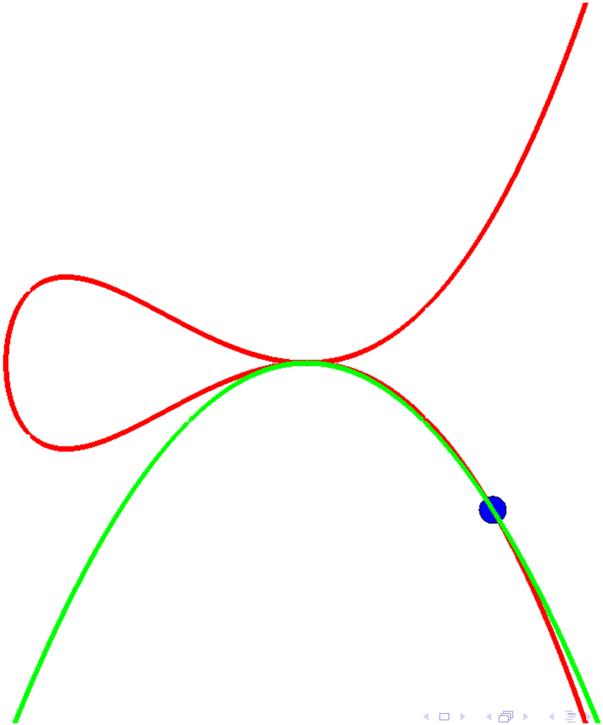


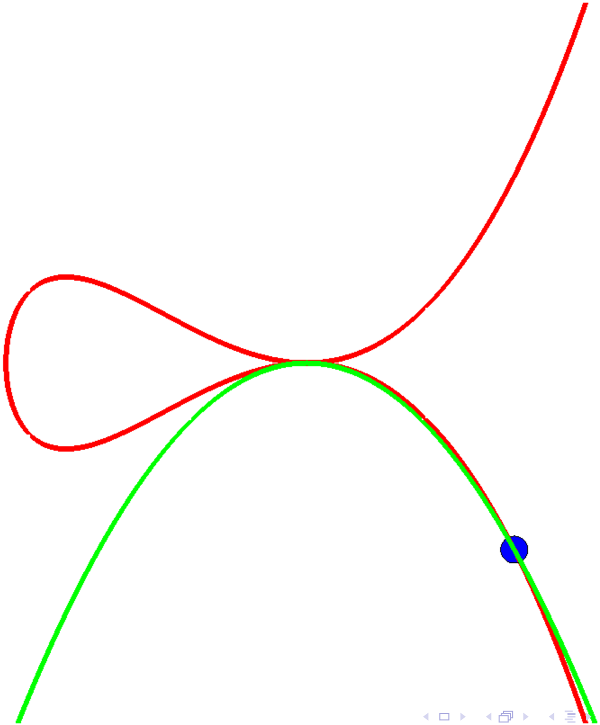


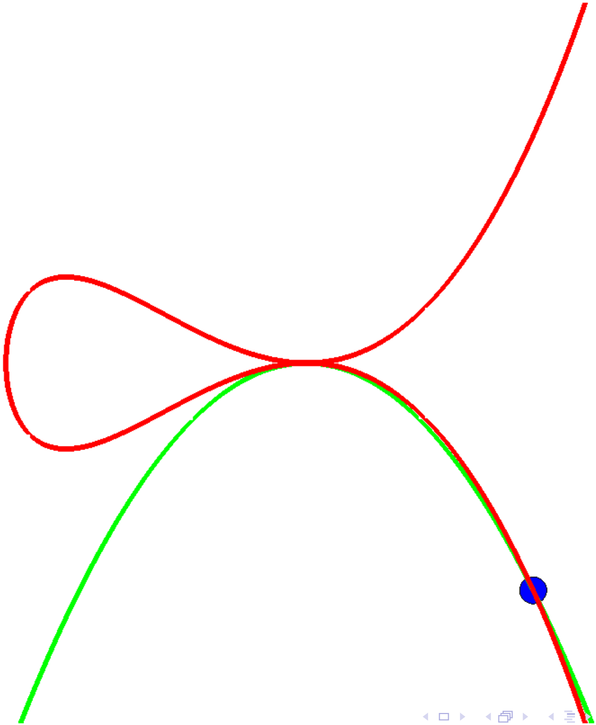


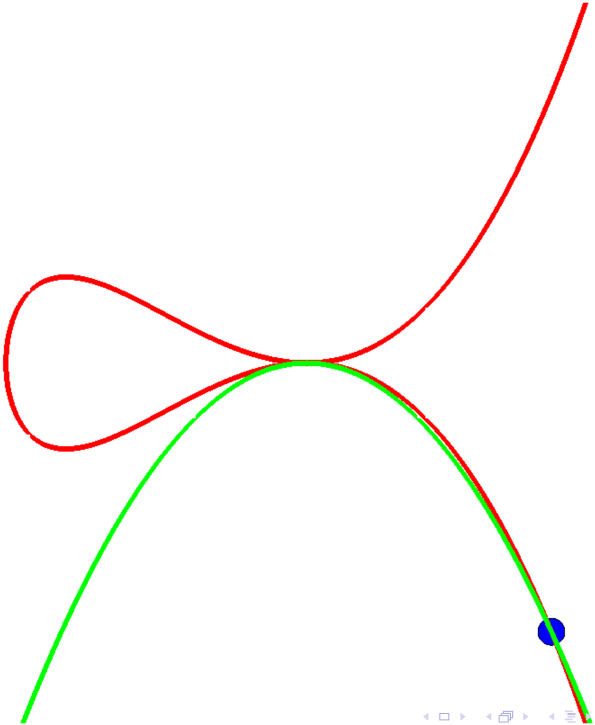


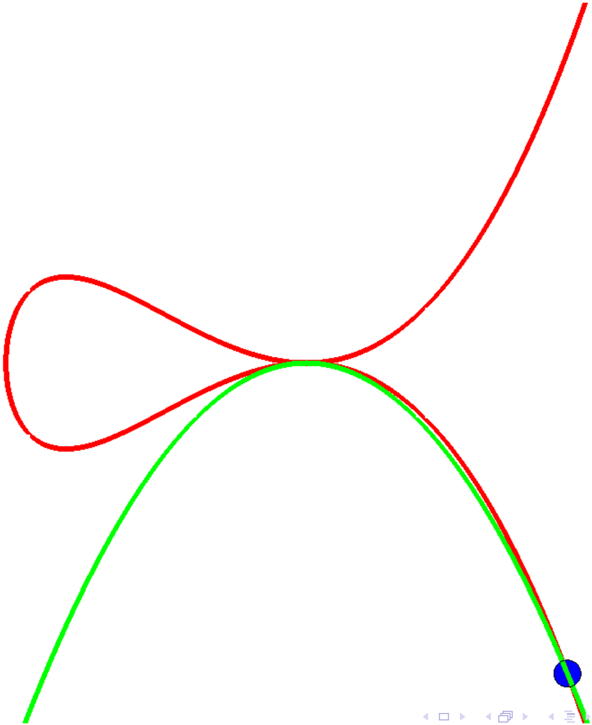


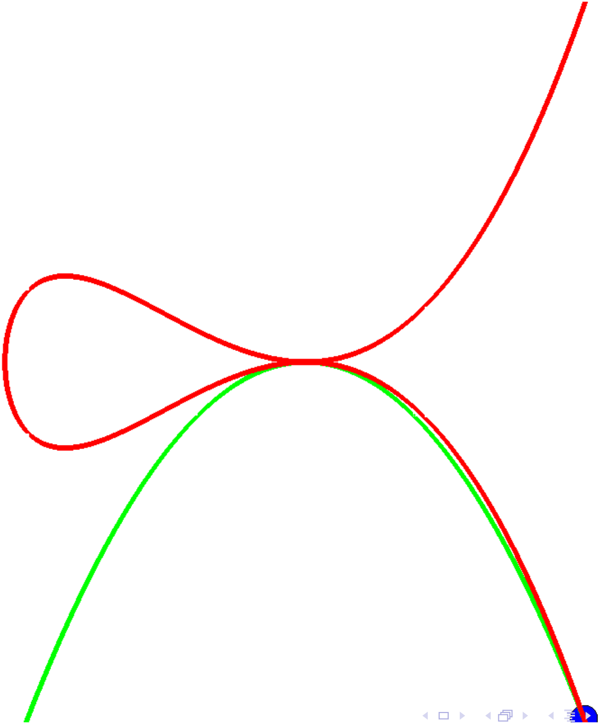


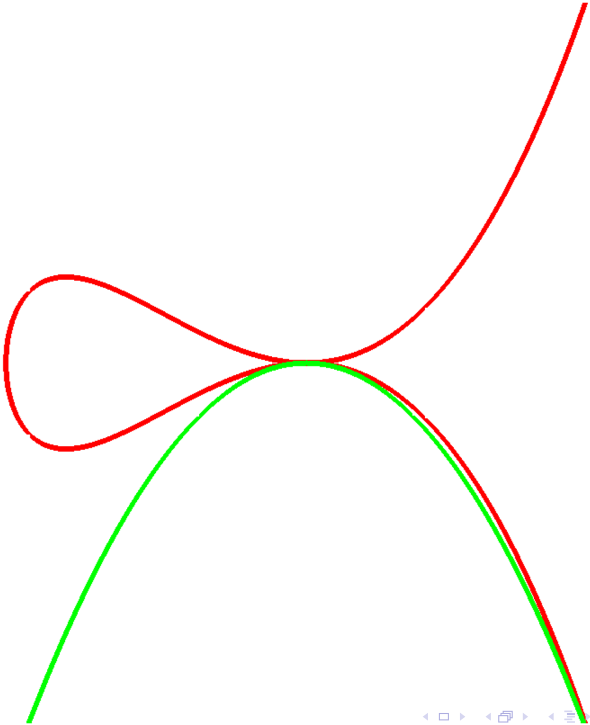


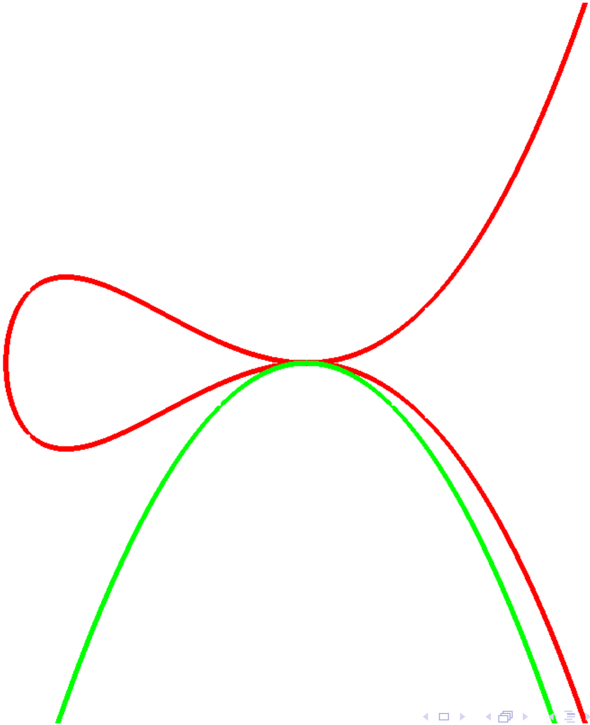


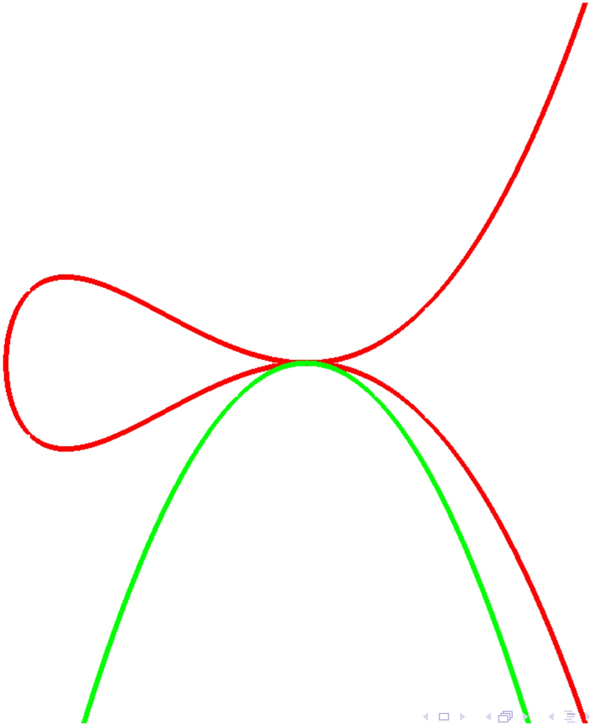


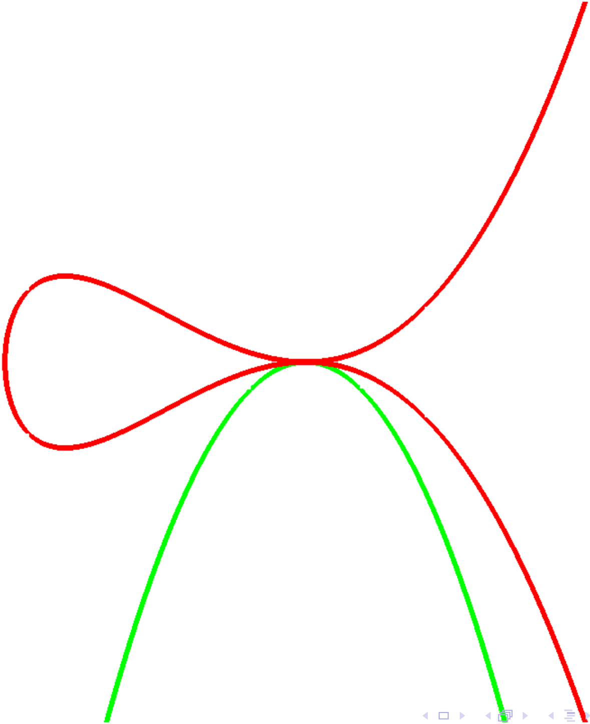


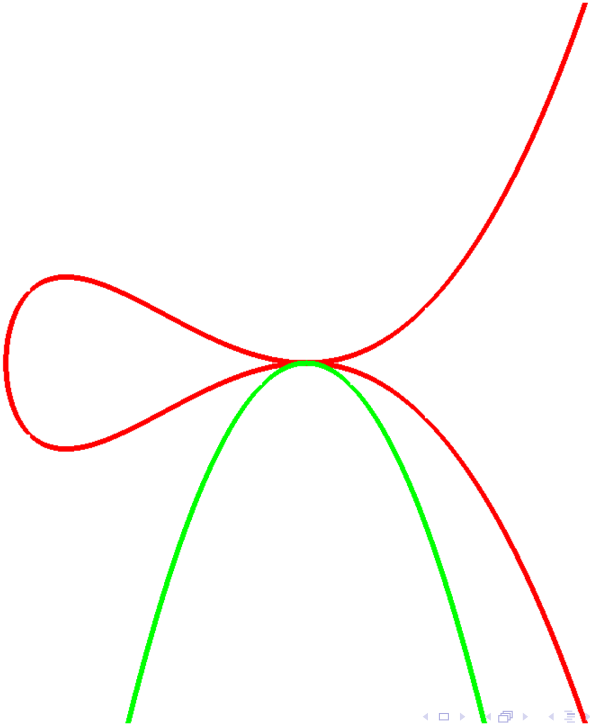


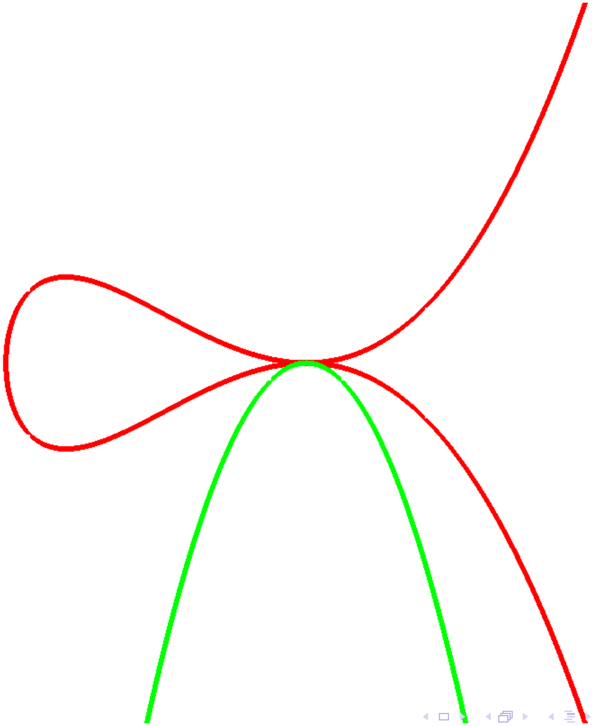


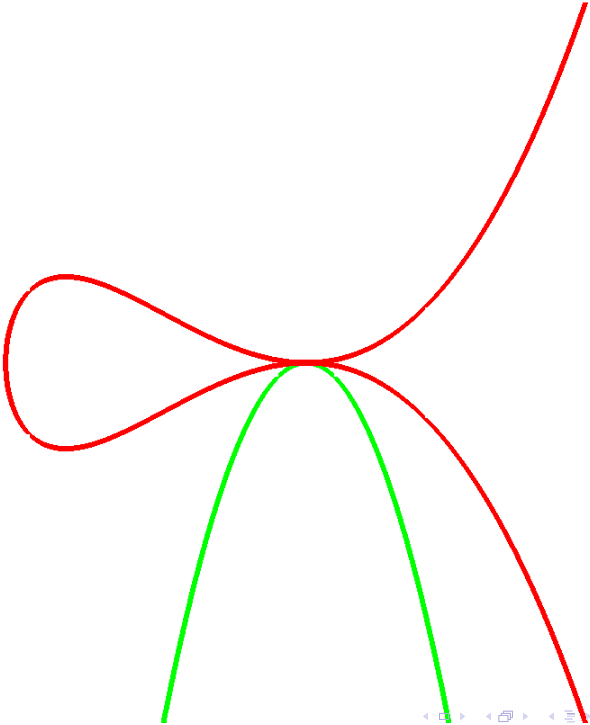


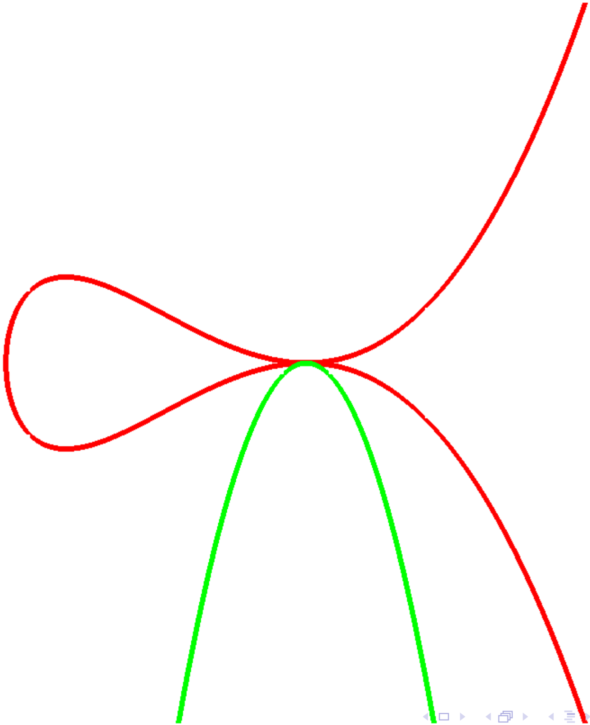


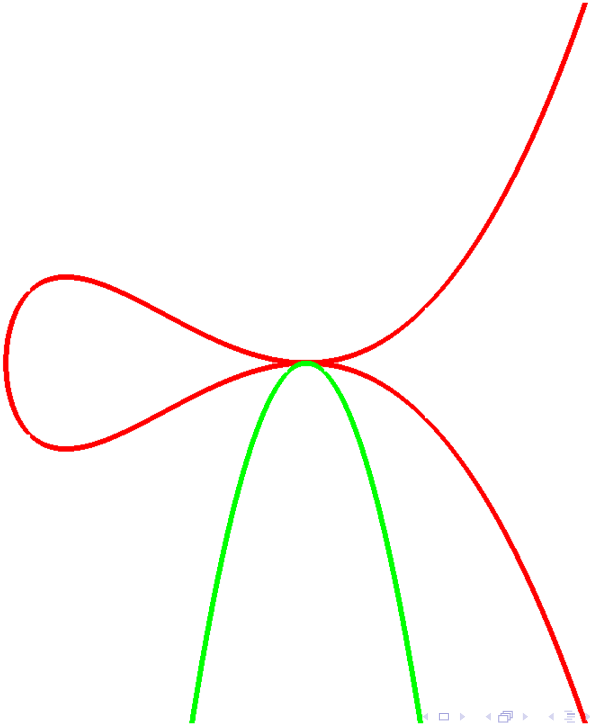


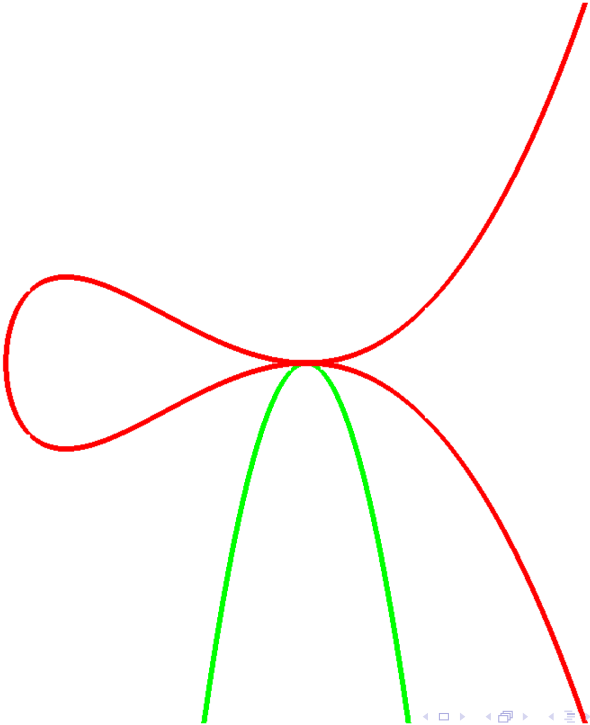


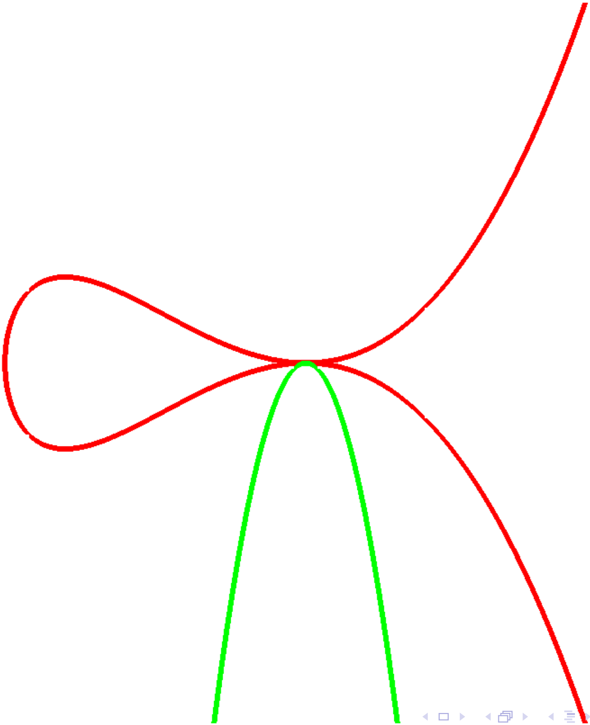


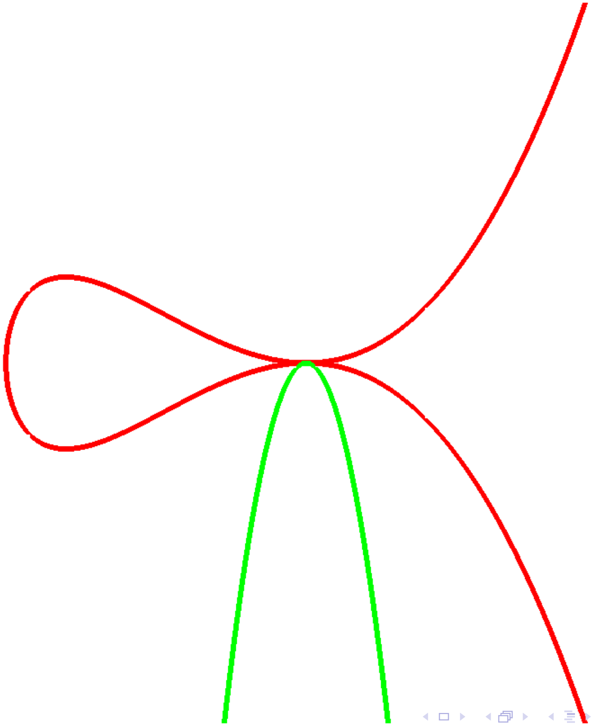


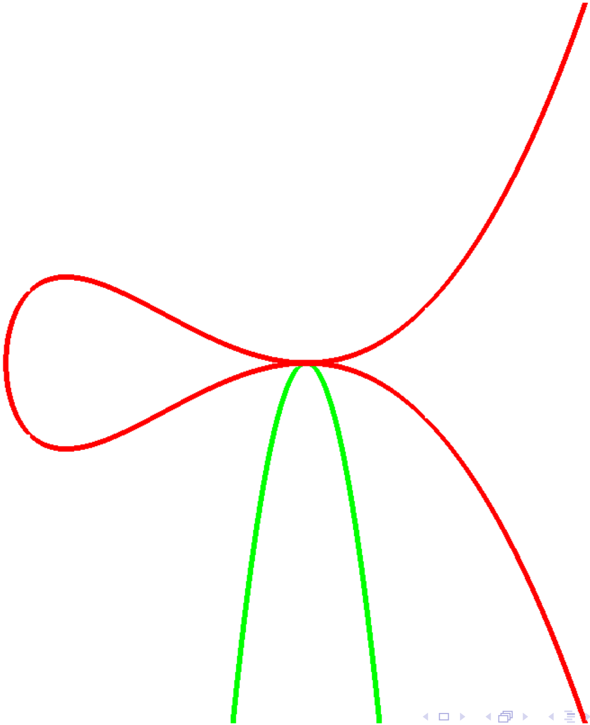


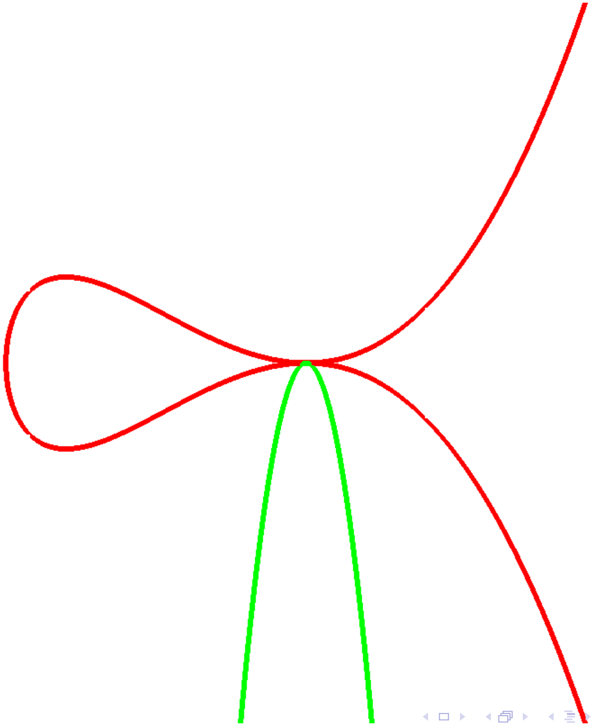


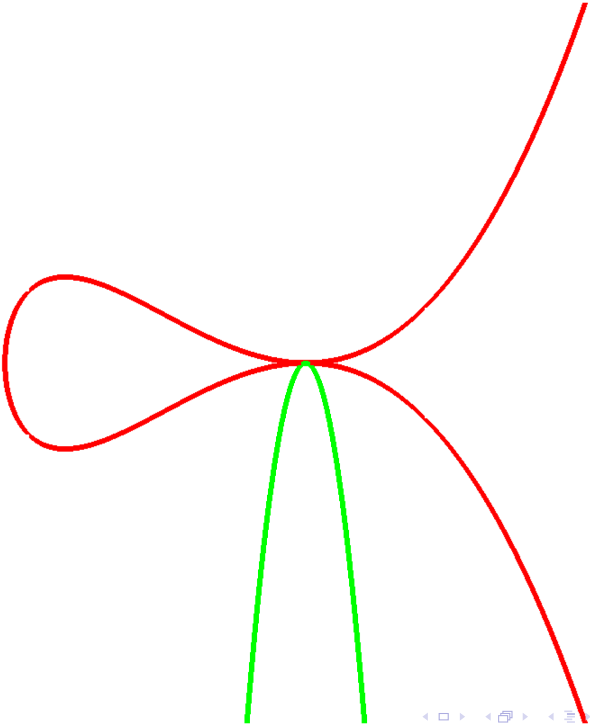


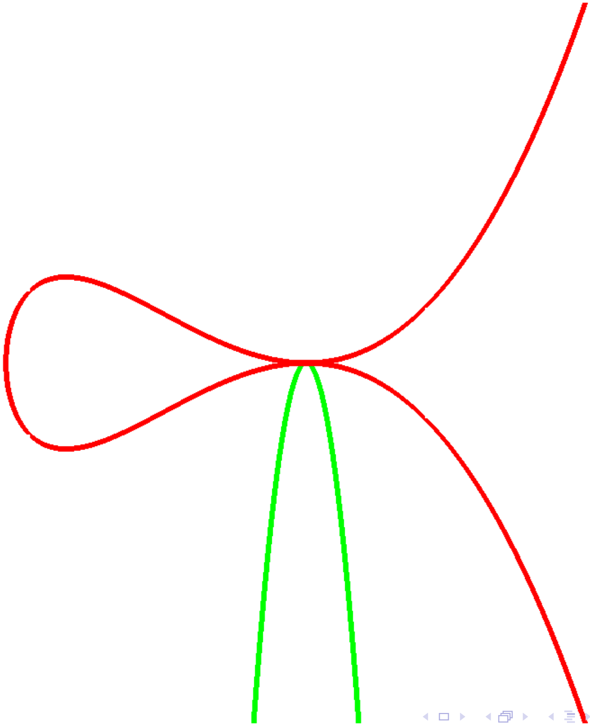


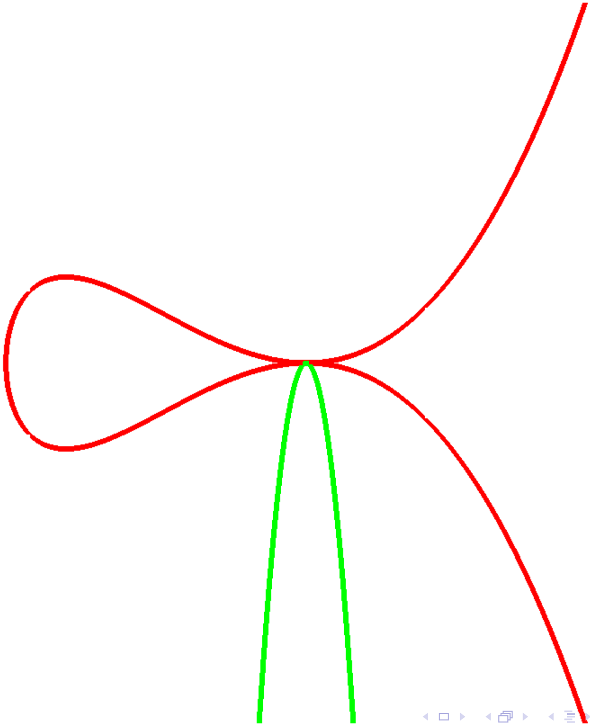


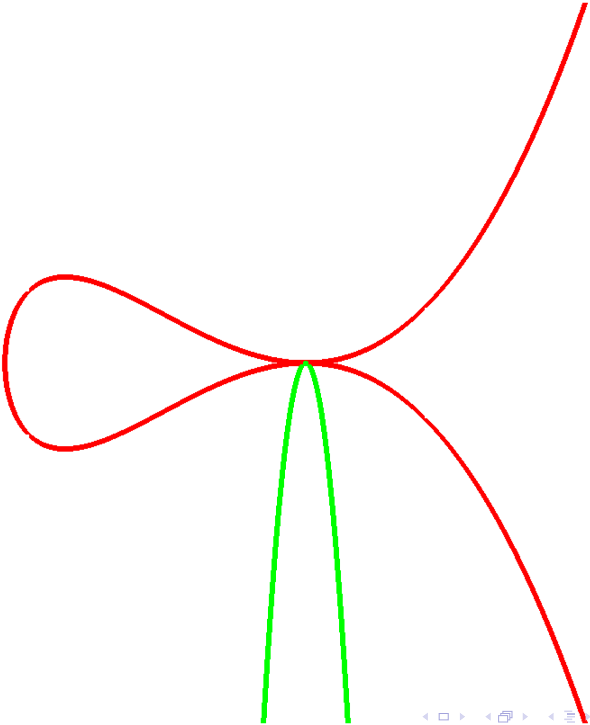


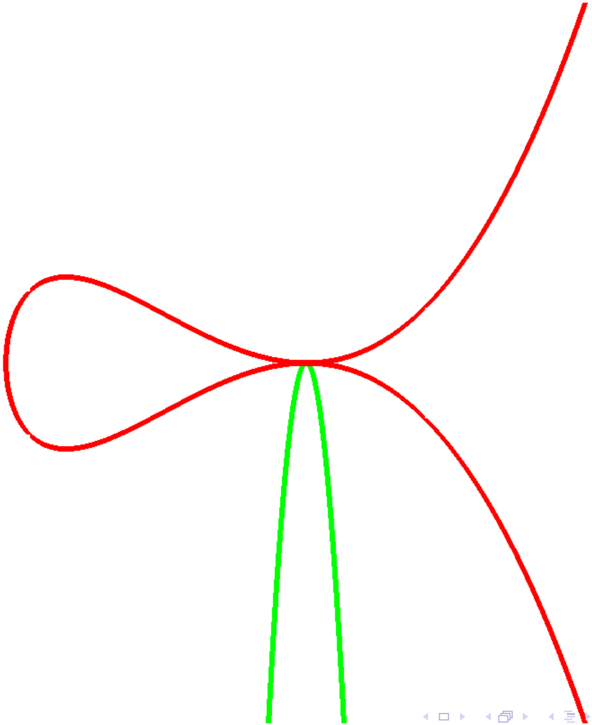


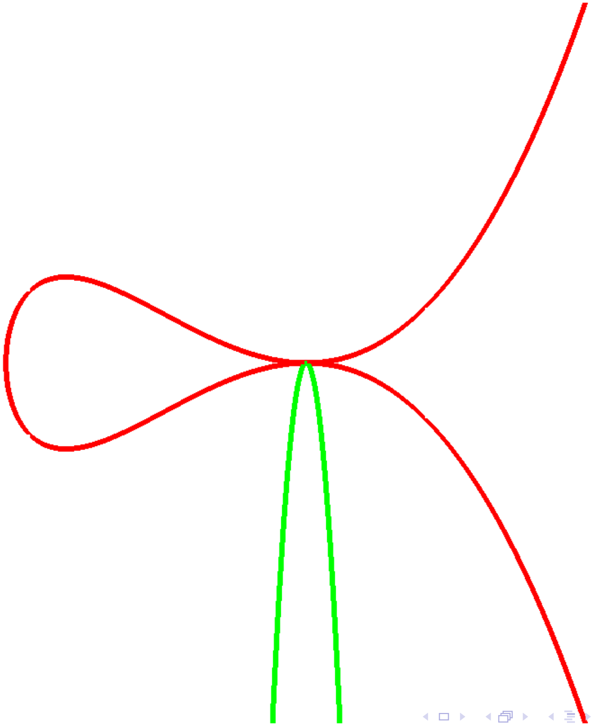


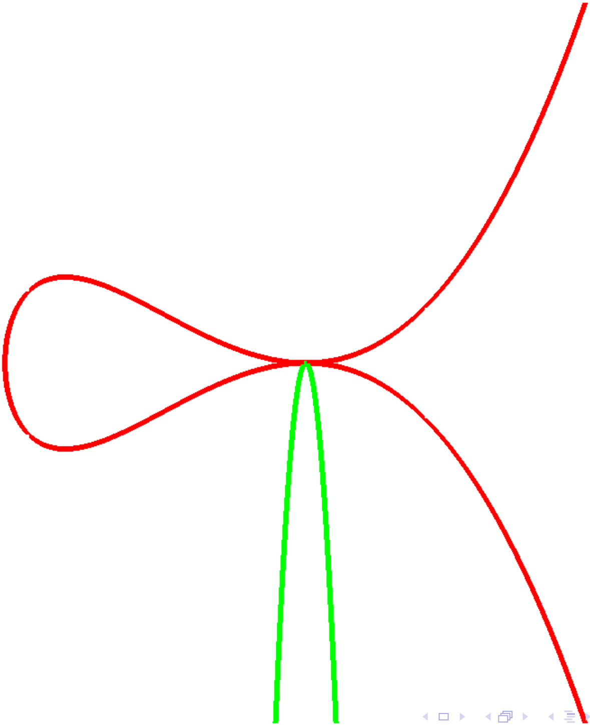


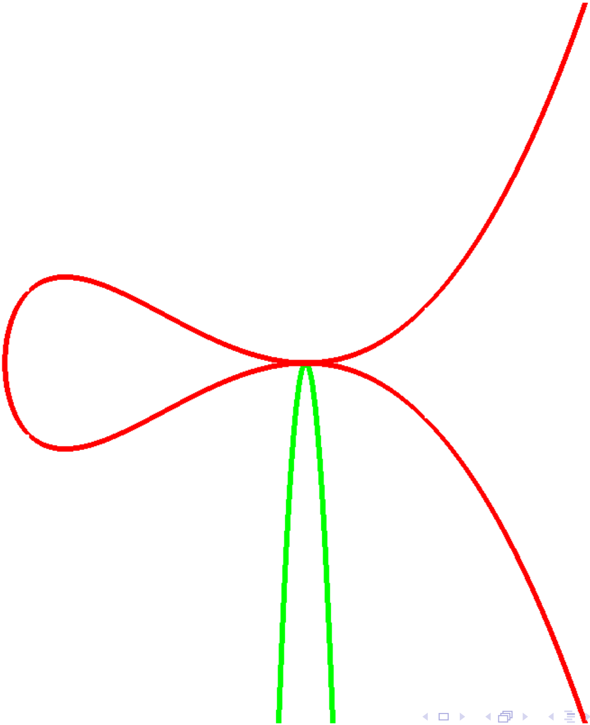


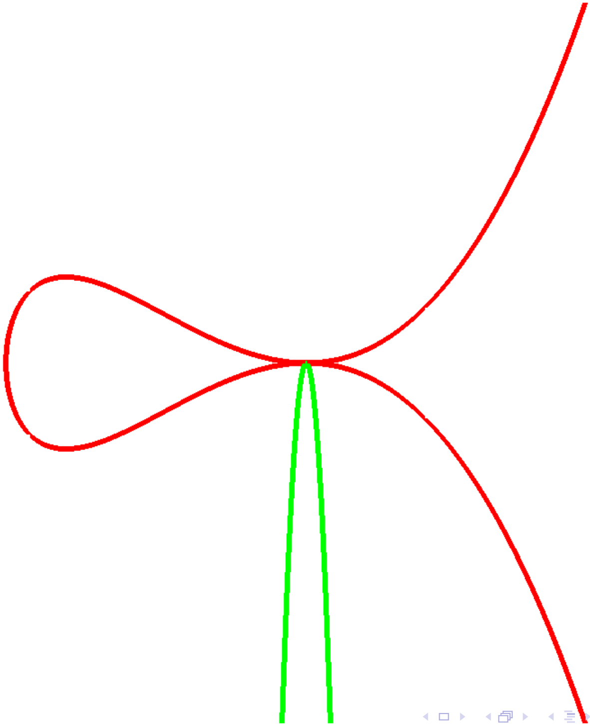


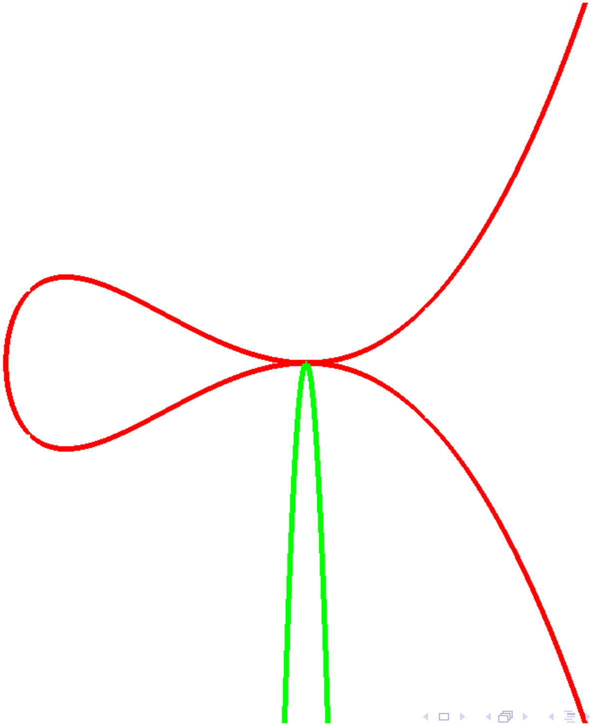


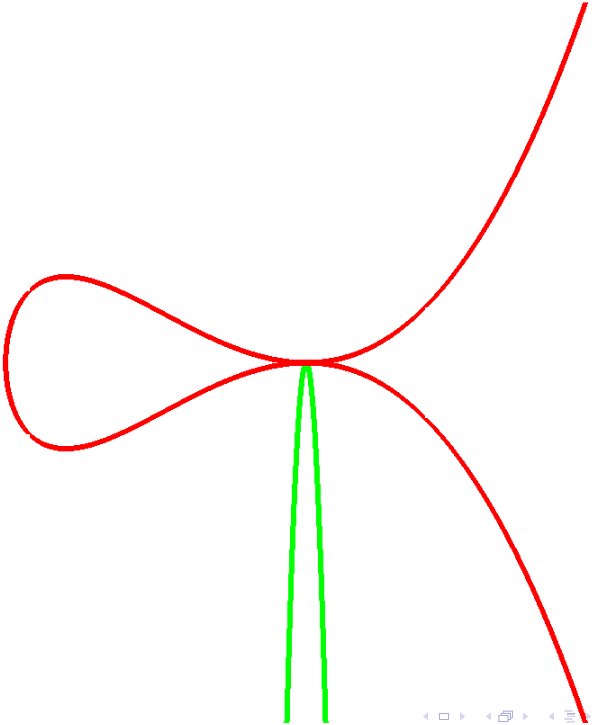


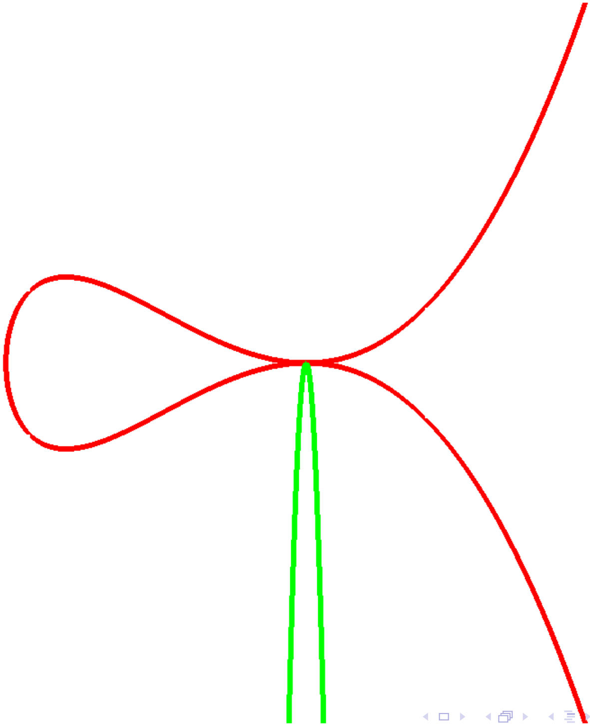


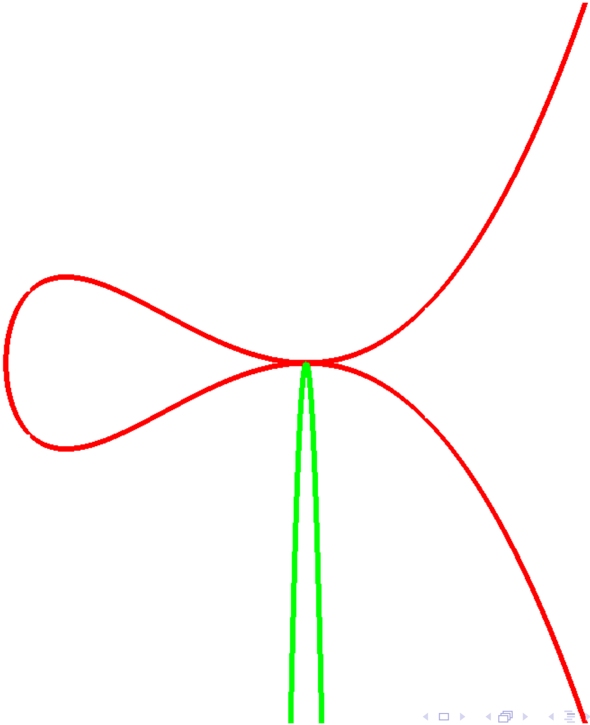


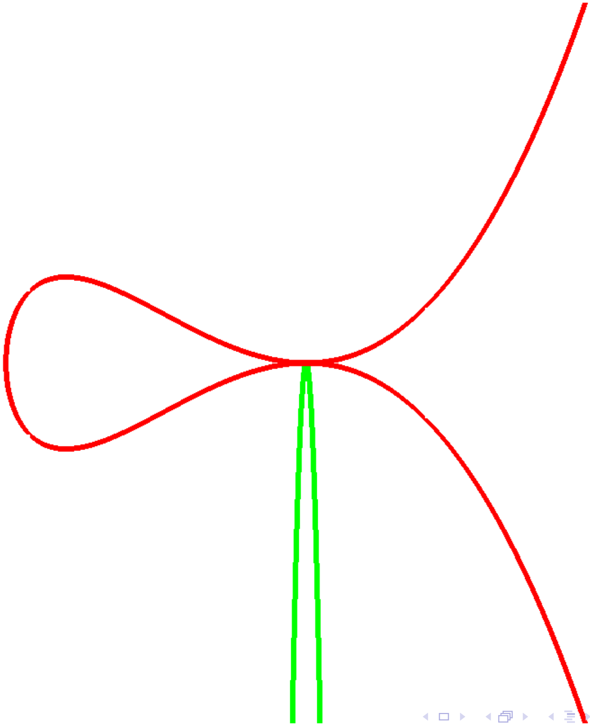


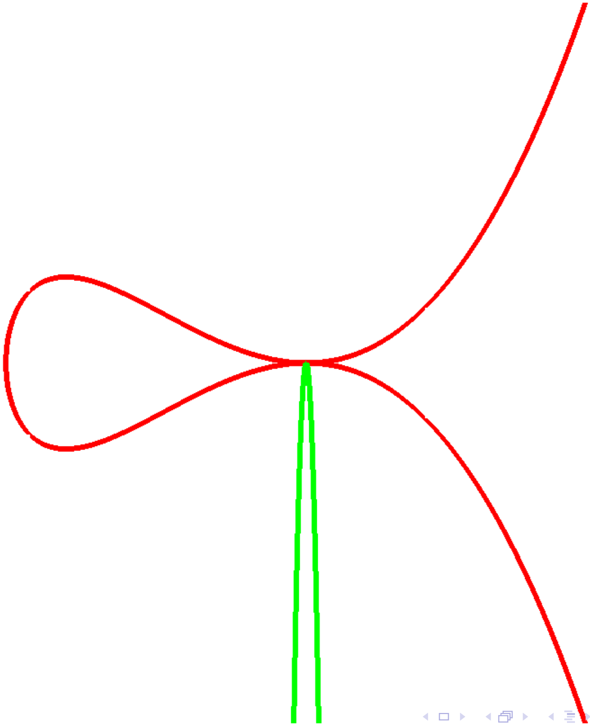


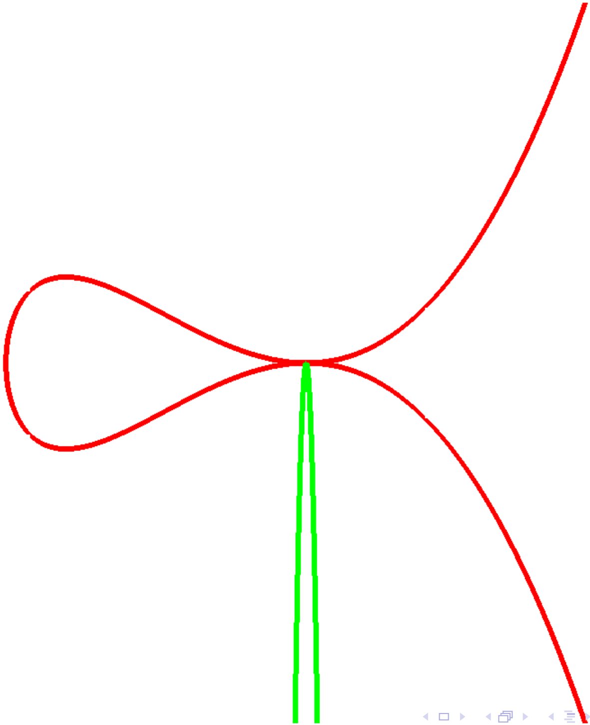


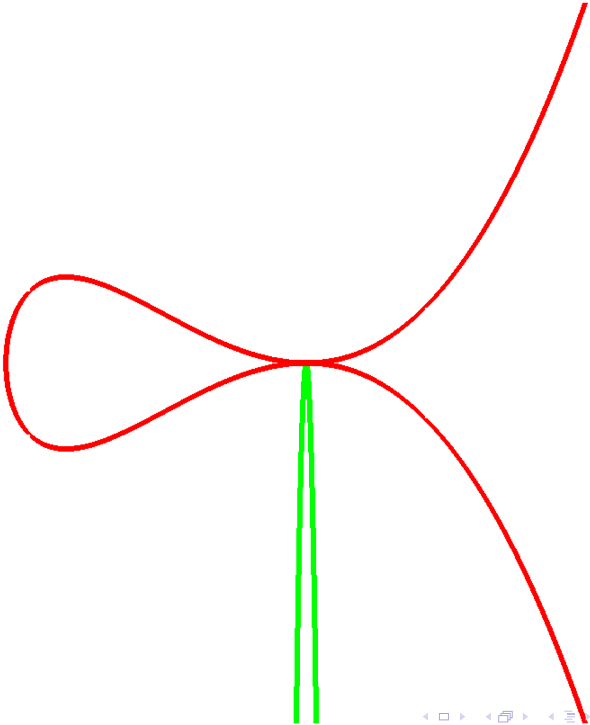


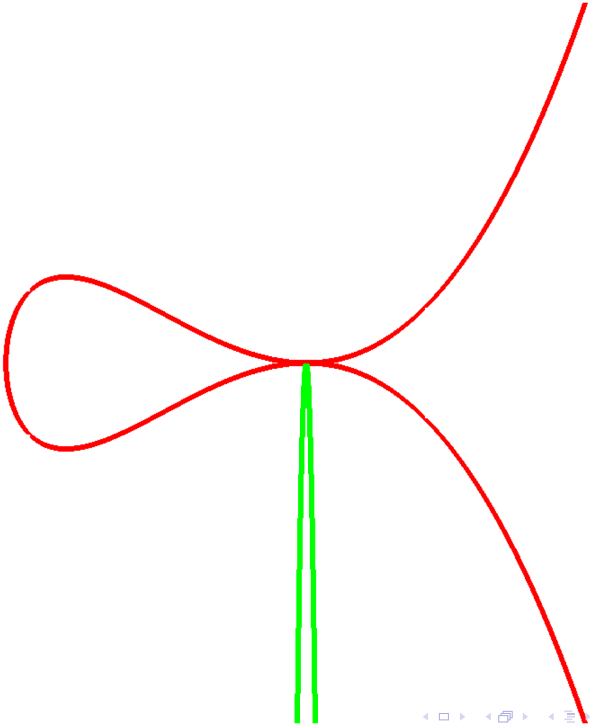


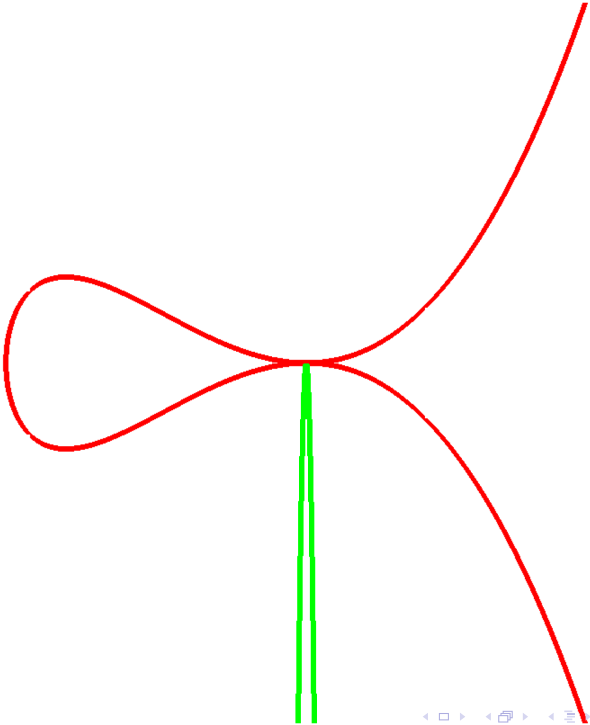


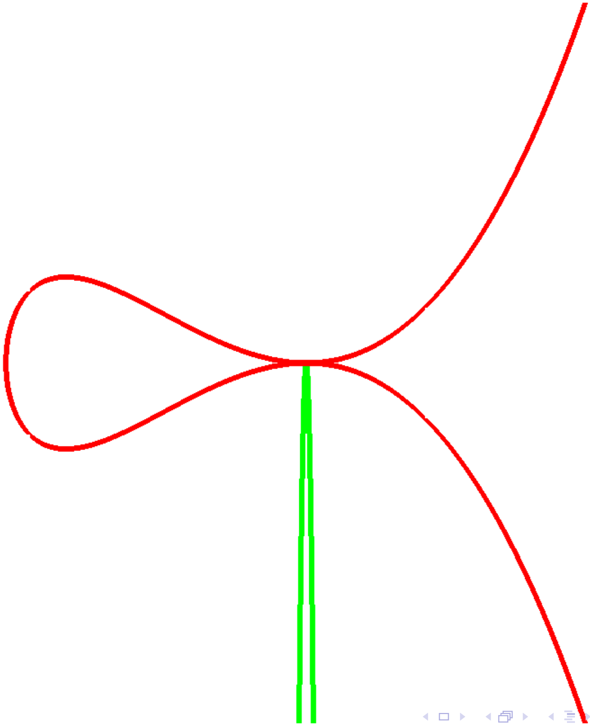


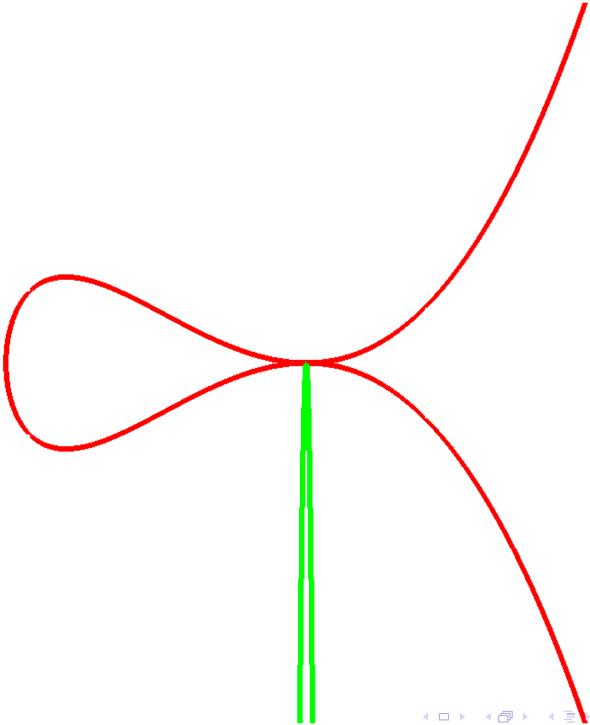


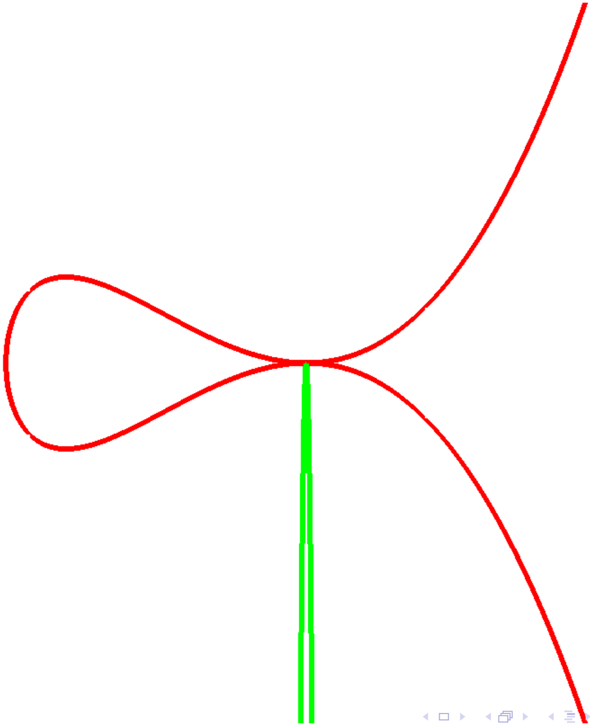


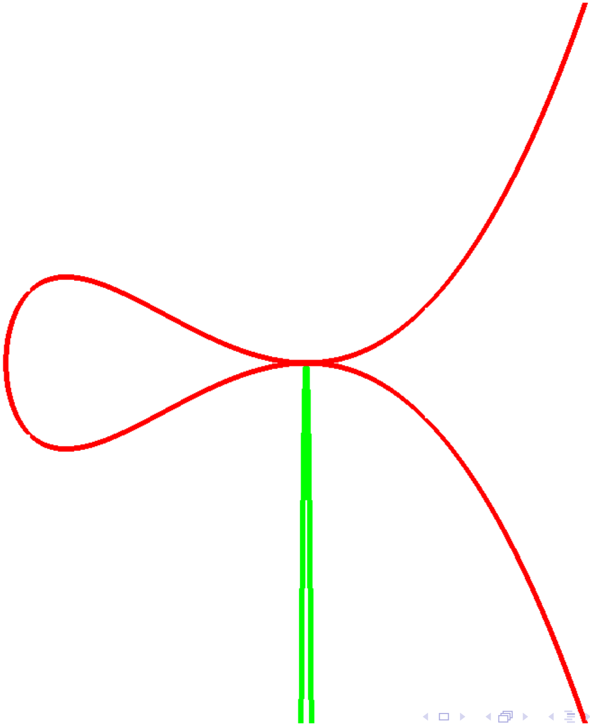


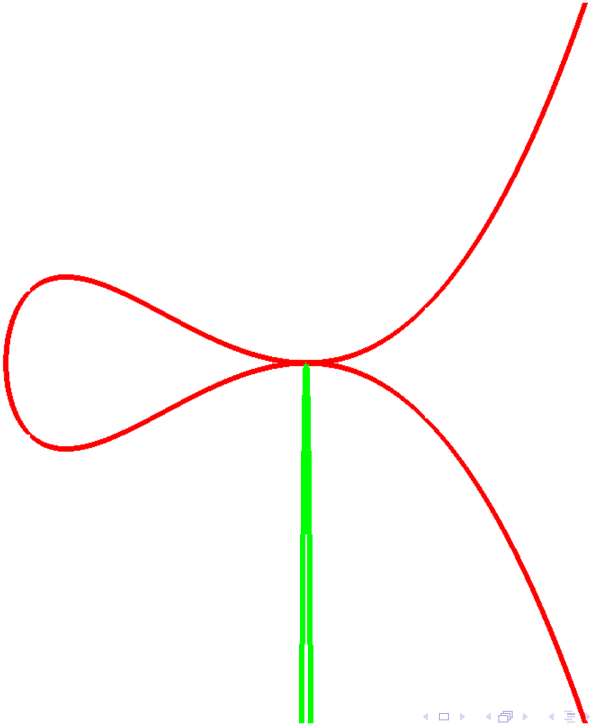


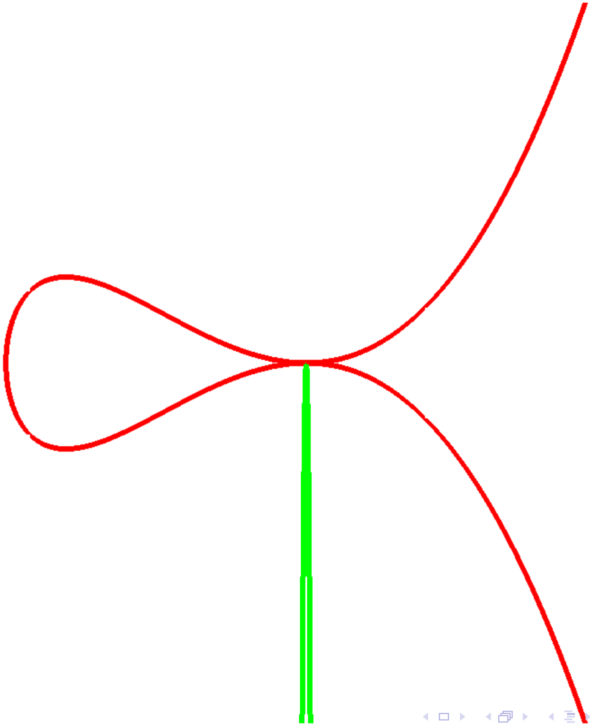


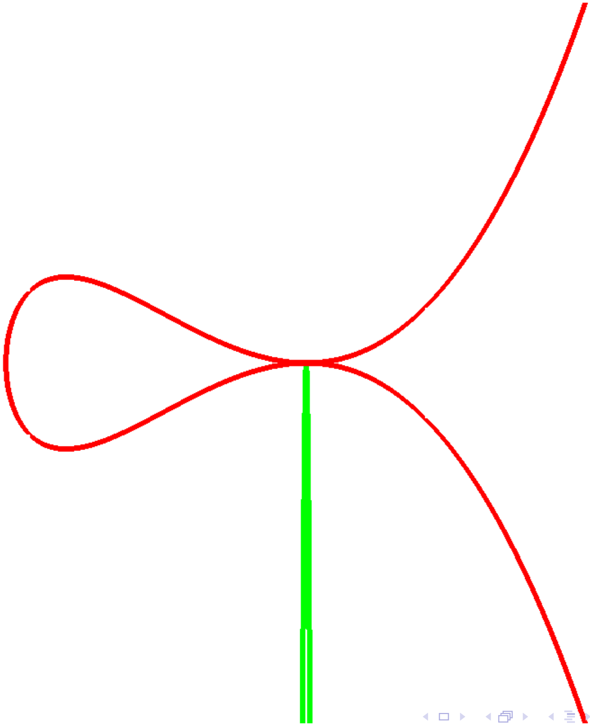


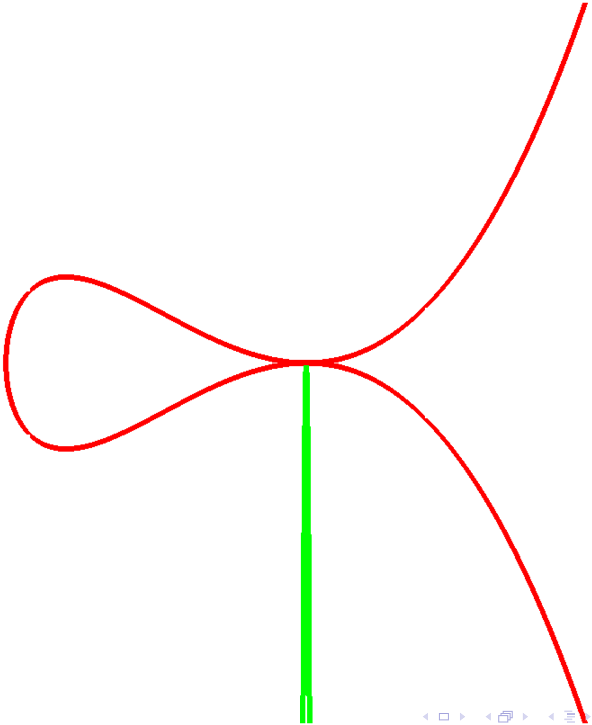


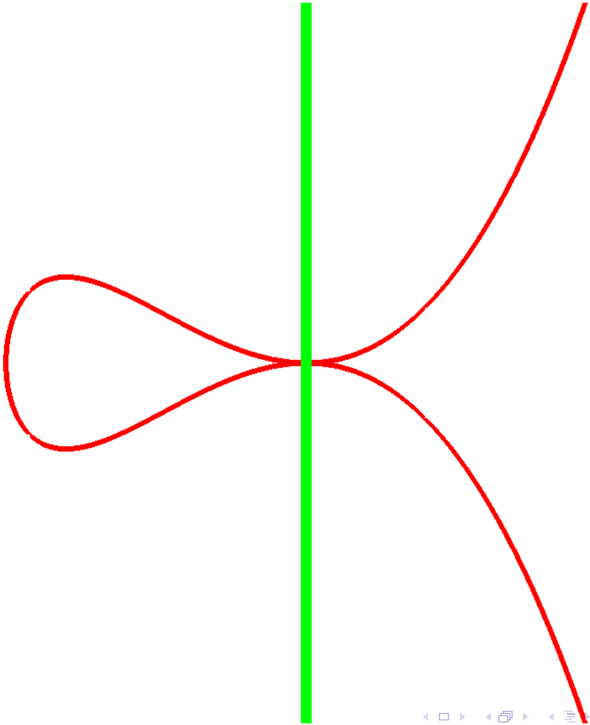


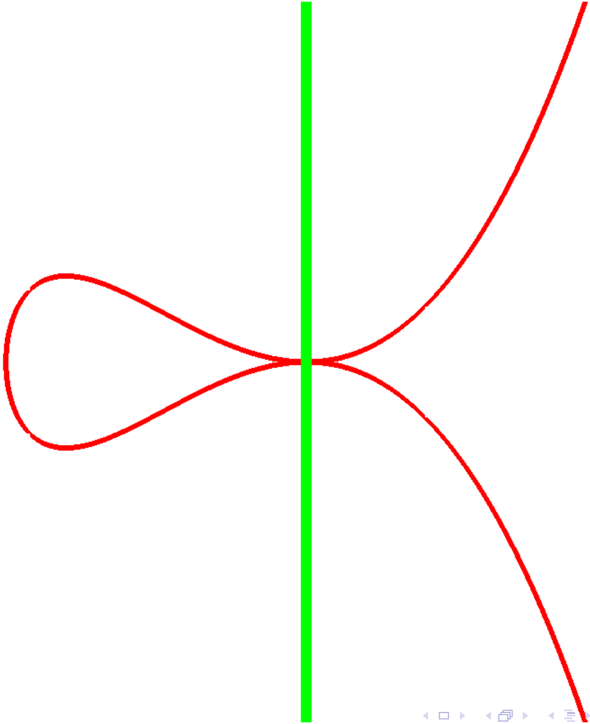












Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$).

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$). If $J = \sqrt{J}$ then the P_i are prime.

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$). If $J = \sqrt{J}$ then the P_i are prime.

For simplicity assume again that $V(I)$ is a curve.

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$). If $J = \sqrt{J}$ then the P_i are prime.
For simplicity assume again that $V(I)$ is a curve.

Theorem (BDLSS, 2013)

Suppose

$$J = \sqrt{\mathrm{Jac}(I) + I} = P_1 \cap \ldots \cap P_r$$

with prime ideals P_i,

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$). If $J = \sqrt{J}$ then the P_i are prime.
For simplicity assume again that $V(I)$ is a curve.

Theorem (BDLSS, 2013)

Suppose

$$J = \sqrt{\operatorname{Jac}(I) + I} = P_1 \cap \ldots \cap P_r$$

with prime ideals P_i, and $A \subset B_i \subset \overline{A}$ is the ring given by the normalization algorithm applied to P_i instead of J

Local Techniques for Normalization

Similarly to the prime factorization of integers, any ideal $J \subset K[x_1, \ldots, x_n]$ has a **primary decomposition** as an intersection

$$J = P_1 \cap \ldots \cap P_r$$

of **primary ideals** P_i (i.e. $ab \in P_i \Rightarrow a \in P_i$ or $\exists m : b^m \in P_i$). If $J = \sqrt{J}$ then the P_i are prime.
For simplicity assume again that $V(I)$ is a curve.

Theorem (BDLSS, 2013)

Suppose

$$J = \sqrt{\mathrm{Jac}(I) + I} = P_1 \cap \ldots \cap P_r$$

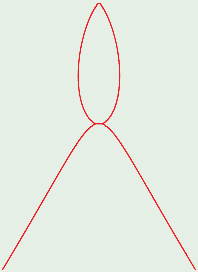
with prime ideals P_i, and $A \subset B_i \subset \overline{A}$ is the ring given by the normalization algorithm applied to P_i instead of J, then

$$\overline{A} = B_1 + \ldots + B_r$$

Local Techniques for Normalization

Example

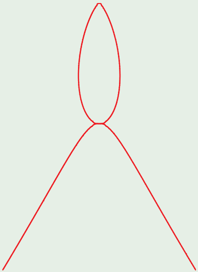
For $I = \langle x^4 + y^2(y-1)^3 \rangle$



Local Techniques for Normalization

Example

For $I = \langle x^4 + y^2(y-1)^3 \rangle$



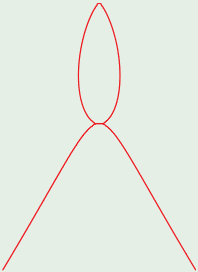
we have

$$J = \langle x, y \rangle \cap \langle x, y-1 \rangle$$

Local Techniques for Normalization

Example

For $I = \langle x^4 + y^2(y-1)^3 \rangle$



we have

$$J = \langle x, y \rangle \cap \langle x, y-1 \rangle$$

and $\overline{A} = B_1 + B_2$ with

$$B_1 = \left\langle 1,\ \frac{x^2}{y}, \frac{x^4}{y^2} \right\rangle \qquad B_2 = \left\langle 1,\ \frac{x^2}{y-1},\ \frac{x^3}{(y-1)^2} \right\rangle$$

References

- D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms*, Springer (2007)
- G.-M. Greuel, G. Pfister, *A Singular introduction to commutative algebra*, Springer (2008)
- H. Schenck, *Computational algebraic geometry*, Cambridge (2003)

- M. Reid, *Undergraduate algebraic geometry* Cambridge (1988)
- M. Reid, *Undergraduate commutative algebra* Cambridge (1995)
- D. Eisenbud, *Commutative algebra - With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer (1995)

References

- J. Boehm, W. Decker, S. Laplagne, G. Pfister, A. Steenpaß, S. Steidel, *Parallel algorithms for normalization*, J. Symbolic Comput. (2013)
- J. Boehm, W. Decker, M. Schulze, *Local analysis of Grauert-Remmert type normalization algorithms*, Internat. J. Algebra Comput. (2014)

- Th. de Jong, *An algorithm for computing the integral closure*, J. Symbolic Comput. (1998)
- G.-M. Greuel, S. Laplagne, F. Seelisch, *Normalization of rings*, J. Symbolic Comput. (2010)
- W. Vasconcelos, *Integral Closure*, Springer (2005)
- I. Swanson, C. Hunecke, *Integral Closure of Ideals, Rings, and Modules* Cambridge (2006)